gettechnical

EDUCATION FOR FINANCIAL INSTITUTIONS

SAR Handbook

Presented by: Gettechnical Inc

(800) 354-3051 | gettechnicalincorporated@gmail.com | www.gettechnicalinc.com

Visit our website to order manuals, view live feeds, and get information about upcoming seminars!

www.gettechnicalinc.com

The material used in this text has been drawn from sources believed to be reliable. Every effort has been made to assure the accuracy of the material; however, the accuracy of this information is not guaranteed. The laws are often changed without prior notice from the government. The SAR 2021 Manual is sold with the understanding that the publisher and the editor are not engaging in the practice of law or accounting. We are not responsible for the actions of your company's employees.

The text is designed to address most deposit account documentation issues. However, you will wish to consult your attorney when you are unsure of an answer.

Published by:
gettechnical inc.

P.O. Box 790
Covington, VA 24426
and
4417 13th Street PMB 310
Saint Cloud, FL 34769
Office 1-800-354-3051
E-mail: **gettechnicalincorporated@msn.com**
Website: **www.gettechnicalinc.com**

All rights reserved. This material may not be reproduced in whole or in part in any form or by any means without written permission from the publisher.

Printed in the United States of America.

© Gettechnical Inc. 2021

INSTRUCTOR

Deborah Crawford is the President of gettechnical inc, a Virginia -based firm, specializing in the education of banks and credit unions across the nation. Her 30+ years of banking and teaching experience began at Hibernia National Bank in New Orleans. She graduated from Louisiana State University with both her bachelor's and master's degrees. Deborah's specialty is in the deposit side of the financial institution where she teaches seminars on regulations, documentation, insurance and Individual Retirement Accounts.

gettechnicalincorporated@gmail.com (e-mail)
www.gettechnicalinc.com (website)

© gettechnical inc 2021

TABLE OF CONTENTS

FORM AND INSTRUCTIONS 7

FINCEN FORM SAR ATTACHMENT D – ELECTRONIC FILING INSTRUCTIONS 8
FINCEN FORM SUSPICIOUS ACTIVITY REPORT (VERSION 1.2 / 6/22/18) 48
OVERVIEW OF FINCEN SAR CHANGES 55

FILINGS, CORRECTED, CONTINUING, AMENDED AND JOINT FILINGS 63

FILING REPORTS: 64
CORRECTED/AMENDED REPORTS 65
CONTINUING REPORTS: 66
JOINT REPORT 67

INFORMATION ON SUBJECTS 71

INSTRUCTIONS ASK FOR MORE DETAILED INFORMATION 72
GATHERING THE INFORMATION AT NEW ACCOUNTS 74
FORM: CONSUMER PROFILE 75
FORM: LEGAL ENTITY PROFILE 78
FORM: BSA REFERRAL 86
FORM: BSA REFERRAL FOR MORTGAGES 91

THE NARRATIVE 95

THE NARRATIVE 96
SPREADSHEET 100

WHEN TO FILE AND WHEN TO NOT FILE 101

BSA SAR FILING INSTRUCTIONS: 102

FRONTLINE AND SYSTEM RED FLAGS 105

TRACK ONE: FRONTLINE 107
BSA INCIDENT REPORT (2018 CHANGES) 118
TRACK TWO: SYSTEMS 120

THE INVESTIGATION 141

IDENTIFYING UNDERLYING CRIME 142
SAR DECISION MAKING 149
NEW LAW EFFECTIVE JANUARY 3, 2011 MAY SUPERSEDE SOME GUIDANCE IN BSA EXAM MANUAL ON CONFIDENTIALITY AND DISCLOSURE 153
SHARING SARS WITH HEAD OFFICES AND CONTROLLING COMPANIES 155
SAR IMPORTANCE TO LAW ENFORCEMENT 156
SAR ISSUES AND GUIDANCE: DATE OF "INITIAL DETECTION" AND THE 30-DAY SAR CLOCK 157
INVESTIGATION WORKSHEET 160
TIPS FROM THE REGULATORS 161

© gettechnical inc 2021

SAR NARRATIVES 163
30-DAY TIME PERIOD IN WHICH TO FILE A SUSPICIOUS ACTIVITY REPORT 163

CONFIDENTIALITY 165
SAFE HARBOR: OUT OF THE INSTRUCTIONS 166
PROHIBITION ON NOTIFICATION 168
SARS GUIDANCE AS TO WHAT TO DO WHEN ASKED FOR PRODUCTION OF SUSPICIOUS ACTIVITY REPORTS 170
LAW ENFORCEMENT INQUIRIES AND REQUESTS 172
SAR FILING AFTER LAW ENFORCEMENT NOTIFICATION 173
FINCEN ADVISORY: SAR CONFIDENTIALITY REMINDER FOR INTERNAL AND EXTERNAL COUNSEL OF FINANCIAL INSTITUTIONS (ISSUED 3/2/12) 174
FINCEN – GUIDANCE ON SAR SUPPORTING DOCUMENTATION 177
SAR FILING OUTSIDE OF THE UNITED STATES 180
OFFICE OF FOREIGN ASSETS CONTROL (OFAC) 182
NATIONAL SECURITY LETTERS (NSLS) AND SARS 183

MISCELLANEOUS 185
ANSWERS TO FREQUENLTY ASKED QUESTIONS REGARDING SUSPICIOUS ACTIVITY REPORTING AND OTHER ANTI-MONEY LAUNDERING CONSIDERATIONS (1-19-2021) 186
DEPARTMENT OF FINANCIAL SERVICES: BANKING DIVISION TRANSACTION MONITORING AND FILTERING PROGRAM REQUIREMENTS AND CERTIFICATIONS 191
CFPB ET AL: INTERAGENCY GUIDANCE ON PRIVACY LAWS AND REPORTING FINANCIAL ABUSE OF OLDER ADULTS (9/24/13) 198
CFPB BLOG: BANKS CAN HELP SPOT ELDER FINANCIAL EXPLOITATION AND ABUSE (9/24/13) 203
FINCEN: 2012 SAR DATA REVEALS DROP IN MORTGAGE FRAUD (8/20/13) 204
FINCEN: SUSPICIOUS ACTIVITY RELATED TO MORTGAGE LOAN FRAUD (8/16/12) 206
FINCEN BSA FAQ (UPDATED DECEMBER 2017) 211
FAQS REGARDING THE FINCEN SAR (4/1/13) 220
FINCEN FIN-2018-A003: ADVISORY ON HUMAN RIGHTS ABUSES ENABLED BY CORRUPT SENIOR FOREIGN POLITICAL FIGURES AND THEIR FINANCIAL FACILITATORS (6/12/2018) 231
FINCEN FIN-2018-A001: ADVISORY ON THE FATF-IDENTIFIED JURISDICTIONS WITH AML/CFT DEFICIENCIES (NORTH KOREA INFORMATION ONLY) (2/9/2018) 246
FINCEN FIN-2017-A008: ADVISORY ON NORTH KOREA'S USE OF THE INTERNATIONAL FINANCIAL SYSTEM (11/2/2017) 253
FINCEN FIN-2017-A007: ADVISORY TO FINANCIAL INSTITUTIONS REGARDING DISASTER-RELATED FRAUD (10/31/2017) 264
FINCEN FIN-2017-A003: ADVISORY TO FINANCIAL INSTITUTIONS AND REAL ESTATE FIRMS AND PROFESSIONALS (8/22/2017) 268
FINCEN ADVISORY: FIN-2016-A005 CYBER CRIMES (OCTOBER 25, 2016) 276
FINCEN FIN-2016-A003: ADVISORY TO FINANCIAL INSTITUTIONS ON E-MAIL COMPROMISE FRAUD SCHEMES (9/6/2016) 285
FINCEN ADVISORY: FIN-2014-A008 GUIDANCE ON RECOGNIZING ACTIVITY THAT MAY BE ASSOCIATED WITH HUMAN SMUGGLING AND HUMAN TRAFFICKING – FINANCIAL RED FLAGS (9/11/14) 294
FINCEN ADVISORY: FIN-2014-A005 FUNNEL ACCOUNTS (5/28/14) 305
FINCEN FIN-2012-A009: SUSPICIOUS ACTIVITY RELATED TO MORTGAGE LOAN FRAUD

© gettechnical inc 2021

(8/16/2012) **309**
FINCEN GUIDANCE FIN-2012-G002 : FILING FINCEN'S NEW CURRENCY TRANSACTION REPORT AND SUSPICIOUS ACTIVITY REPORT (3/29/12) **313**
FINCEN ADVISORY FIN-2011-A003 ADVISORY TO FINANCIAL INSTITUTIONS ON FILING SUSPICIOUS ACTIVITY REPORTS REGARDING ELDER FINANCIAL EXPLOITATION (2/11/11) **318**

COVID **321**
FIN-2020-A007 – UNEMPLOYMENT INSURANCE FRAUD (OCTOBER 13, 2020) **322**
FIN-2020-A005 – CYBERCRIME AND CYBER-ENABLED CRIME (JULY 30, 2020) **326**
FIN-2020-A003 – IMPOSTER SCAMS AND MONEY MULE SCHEMES (JULY 7, 2020) **335**
FINCEN NOTICE (MAY 18, 2020) **343**
FIN-2020-A002 - MEDICAL SCAMS (MAY 18, 2020) **347**
FINCEN -PAYCHECK PROTECTION PROGRAM FAQS (APRIL 13, 2020) **356**
FINCEN NOTICE (APRIL 03, 2020) **358**
FINCEN NOTICE (MARCH 16, 2020) **361**

© gettechnical inc 2021

FORM AND INSTRUCTIONS

© gettechnical inc 2021

Safe Harbor:

Federal law (31 U.S.C. 5318(g)(3)) provides financial institutions complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to a regulatory requirement or on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees, and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure."

Confidentiality of SARs:

A Bank Secrecy Act Suspicious Activity Report (BSA SAR), and any information that would reveal the existence of the BSA SAR (collectively, "SAR information"), are confidential, and may not be disclosed except as specified in 31 U.S.C. 5318(g)(2) and in FinCEN's regulations (31 CFR Chapter X).

Prohibition on Disclosures by Financial Institutions:

Federal law (31 U.S.C. 5318(g)(2)) provides that a financial institution, and its directors, officers, employees, and agents who, pursuant to any statutory or regulatory authority or on a voluntary basis, report suspicious transactions to the government, may not notify any person involved in the transaction that the transaction has been reported. Provided that no person involved in the suspicious activity is notified, 31 CFR Chapter X clarifies that the following activity does not constitute a prohibited disclosure:

• Disclosure of SAR information to certain governmental authorities or other examining authorities that are otherwise entitled by law to receive SAR information or to examine for or investigate suspicious activity;

• Disclosure of the underlying facts, transactions, and documents upon which a BSA SAR is based; and

• For those institutions regulated by a Federal functional regulator (Federal bank regulatory agencies, the Securities and Exchange Commission (SEC), and the

Commodity Futures Trading Commission (CFTC)), the sharing of SAR information within an institution's corporate organizational structure, for purposes that are consistent with the Bank Secrecy Act, as determined by regulation or guidance.

Prohibition on Disclosures by Government Authorities:

© gettechnical inc 2021

Federal law (31 U.S.C. 5318(g)(2)) also provides that an officer or employee of any Federal, state, local, tribal, or territorial government within the United States who has knowledge that such report was made, may not disclose to any person involved in the transaction that the transaction has been reported, other than as necessary to fulfill the official duties of such officer of employee. FinCEN's regulations clarify that "official duties" must be consistent with Title II of the Bank Secrecy Act and shall not include the disclosure of a SAR, or any information that would reveal the existence of a SAR, in response to a request for disclosure of non-public information or a request for use in a private legal proceeding, including a request pursuant to 31 CFR § 1.11.

BSA SAR Filing Instructions:

1. Who Must File: Certain financial intuitions operating in the United States shall file with FinCEN, to the extent and in the manner required by 31 CFR Chapter X and 12 CFR §§ 21.11, 208.62, 353.3, and 748.1, a report of any suspicious transaction relevant to a possible violation of law or regulation. The following financial institutions are required to file a BSA SAR: Banks (31 CFR §1020.320); Casinos and Card Clubs (31 CFR § 1021.320); Money Services Businesses (31 CFR § 1022.320); Brokers or Dealers in Securities (31 CFR § 1023.320); Mutual Funds (31 CFR § 1024.320); Insurance Companies (31 CFR § 1025.320); and Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR § 1026.320).

2. Filing Deadlines: A BSA SAR shall be filed no later than 30 calendar days after the date of the initial detection by the reporting financial institution of facts that may constitute a basis for filing a report. If no suspect is identified on the date of such initial detection, a financial institution may delay filing a BSA SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the financial institution shall immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a BSA SAR. Financial institutions wishing voluntarily to report suspicious transactions that may relate to terrorist activity may call FinCEN's Financial Institutions Hotline at 1-866-556-3974 in addition to filing timely a BSA SAR.

3. Filing Requirements for Financial Institutions: A financial institution must report any transaction that requires reporting under the terms of 31 CFR Chapter X if the transaction is conducted or attempted by, at, or through the financial institution and involves or aggregates at least $5,000 ($2,000 for money services businesses, except as provided in Section 6 of this document) and the financial institution knows, suspects, or has reason to suspect that the transaction or pattern of transactions of which the transaction is a part:

• Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

• Is designed, whether through structuring or other means, to evade any requirement of 31 CFR Chapter X or any other regulation promulgated under the Bank Secrecy Act, Public Law 91-508, as amended, codified at 12 U.S.C 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5332;

© gettechnical inc 2021

• Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or

• Involves the use of the financial institution to facilitate criminal activity.

4. Additional Filing Instructions for Banks: In addition to the above requirements, a bank (as defined in 31 CFR § 1010.100) must file a BSA SAR for activity (as required by 31 CFR § 1020.320 and 12 CFR §§ 21.11, 208.62, 353.3, and 748.1) involving:

• **Insider abuse involving any amount.** Whenever the bank detects any known or suspected Federal criminal violations, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.

• **Violations aggregating $5,000 or more where a suspect can be identified.** Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $5,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an “alias,” then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers’ licenses or social security numbers, addresses and telephone numbers, must be reported.

• **Violations aggregating $25,000 or more regardless of a potential suspect.** Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $25,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

5. Voluntary BSA SAR Filings: Financial institutions may also file with FinCEN a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR Chapter X. A voluntary filing does not relieve a financial institution from the responsibility of complying with any other reporting requirements imposed by the SEC, the CFTC, a self-regulatory organization (SRO) (as defined in section 3(a)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78c (a)(26)), or any Registered Futures Association (RFA) or Registered Entity (RE) (as these terms are defined in the Commodity Exchange Act, 7 U.S.C. 21 and 7 U.S.C. 1a(29)).

6. Exceptions: The following are exceptions to the BSA SAR reporting requirements:

• A bank, casino, broker or dealer in securities (BD), futures commission merchant (FCM), or introducing broker in commodities (IB-C) is not required to file a BSA SAR for a robbery or

© gettechnical inc 2021

burglary committed or attempted against the financial institution when the robbery or burglary is reported to appropriate law enforcement authorities.

• A BSA SAR is not required to be filed for lost, missing, counterfeit, or stolen securities that are reported pursuant to the requirements of 17 CFR § 240.17f-1.

• A BD is not required to file a BSA SAR on violations of any of the Federal securities laws or the rules of a SRO by the BD or any of its officers, directors, employees or other registered representatives, other than a violation of 17 CFR § 240.17a-8 or 17 CFR § 405.4, so long as such violation is appropriately reported to the SEC or an SRO.

• An FCM or an IB-C, or any of its officers, directors, employees or associated persons, is not required to file a BSA SAR for a violation of the Commodity Exchange Act (7 U.S.C. 1 *et seq.)*, the regulations of the CFTC (17 CFR Chapter 1), or the rules of any RFA or RE (as those terms are defined in the Commodity Exchange Act, 7 U.S.C. 21 and 7 U.S.C. 1a(29)), as long as such violation is appropriately reported to the CFTC, an RFA, or RE. This exception does not apply to violations of 17 CFR § 42.2.

• An insurance company is not required to report the submission to it of false or fraudulent information to obtain a policy or make a claim, unless the company has reason to believe that that the false or fraudulent submission relates to money laundering or terrorist financing.

• An issuer of money orders or traveler's checks is not required to report a transaction or pattern of transactions when the transactions were identified through a review of clearance records or other similar records and the transaction amount or aggregated transaction amount involves funds or other assets of less than $5,000.

7. Additional Reporting: The Bank Secrecy Act requires financial institutions to file a Currency Transaction Report (CTR) in accordance with the Department of the Treasury's implementing regulations (31 CFR § 1010.310) whenever a currency transaction exceeds $10,000. If a currency transaction exceeds $10,000 and is otherwise reportable as suspicious activity, the institution must file both a CTR (reporting the currency transaction) and a BSA SAR (reporting the suspicious activity). If a currency transaction is $10,000 or less and is otherwise reportable as a suspicious activity, the institution should only file a BSA SAR. Appropriate records must be maintained in each case.

8. Attachment B – Error Correction Instructions

This attachment identifies the requirements and procedures for correcting FinCEN SAR errors reported to batch filers during the FinCEN SAR acknowledgement process.

Error Categories:

There are two main categories of errors identified in batch files: Schema validation errors that result in automatic rejection of the batch file and data errors that represent errors in data entered for individual elements but may not result in a rejection.

Schema validation errors prevent the batch file from being processed and are considered fatal errors. An example of a schema validation error is a missing required element or an element sequence that does not match the schema. An example of a data error is a required element that contains no value. Data errors are classified as primary or secondary warnings, depending on their importance. Primary warnings are file errors that violate electronic filing requirements or instructions and so degrade FinCEN SAR data quality that they must be corrected. Primary warnings make it difficult for regulators, analysts, and law enforcement investigators to locate the FinCEN SARs in the database or identify the nature and circumstances of the suspicious activity. Examples of such warnings include blank last names or legal names, missing financial institution Employer Identification Numbers, or an invalid entry in the suspicious

© gettechnical inc 2021

activity date field. Attachment A – Error Descriptions identifies primary errors by adding an asterisk (*) to the error code.

Secondary warnings are data errors that violate electronic filing requirements or instructions but have a lesser impact on FinCEN SAR data quality. Examples of secondary errors are ZIP Codes that end in four zeros (e.g. 123450000), missing dates of birth, or invalid telephone numbers.

Correction Requirements:

Filers should immediately correct and resubmit a batch file rejected for fatal errors when notified by FinCEN the batch file was not accepted.

When an accepted batch file contains FinCEN SARs with primary warning errors, those FinCEN SARs must be re-filed as a corrected report with the primary errors and any secondary errors corrected. FinCEN SARs that contain only secondary errors need not be corrected. FinCEN requires that filers prevent all reported errors in their future filings. FinCEN recommends that data error corrections be made no later than 30 days after receiving error notifications.

Furthermore, FinCEN recommends that filers remedy any systemic problems in their electronic submissions within 30 days of receiving error notifications. If technical issues prevent filers from implementing corrections within these time frames, filers should notify FinCEN by writing to:

Financial Crimes Enforcement Network
Office of Domestic Liaison
Data Quality Assessments
P.O. Box 39
Vienna, VA 22183

This correspondence should explain the technical issues involved that prevent meeting the time frame, provide an estimate of when the issues will be resolved, and include a contact name and telephone number.

Correction Procedures:

FinCEN SAR batch files are rejected when they contain fatal format errors. Filers must correct all fatal errors identified in the batch file and resubmit the batch file to BSA E-Filing. Because they were not accepted by FinCEN, initial report FinCEN SARs in the re-submitted batch file are still initial reports. Do not identify FinCEN SARs from a rejected batch file as Amended reports unless they originally were filed as Amended reports.

If errors involve accepted with warning errors in the FinCEN SARs of an accepted batch file, filers should correct all errors and file amended reports on the affected FinCEN SARs using the following procedures:

- Make the corrections to all errors in the FinCEN SARs in the accepted batch file.
- Record “Y” in the <CorrectsAmendsPriorReportIndicator> element under the <Activity Association> element in each FinCEN SAR to be corrected.
- Record in the <EFilingPriorDocumentNumber> element under the <Activity> element the BSA Identifier (from the FinCEN SAR Acknowledgement) that was assigned to the FinCEN SAR being corrected.
- Ensure that the <FilingDateText> element contains a new date.
- Complete all other data in the FinCEN SAR in their entirety.
- Retransmit the corrected FinCEN SAR in a new batch file. Do not re-transmit the original batch file because this will cause duplicate database entries on any FinCEN SARs that were not corrected.

© gettechnical inc 2021

1. Attachment C – Electronic XML Filing Instructions

Safe Harbor: Federal law (31 U.S.C. 5318(g)(3)) provides financial institutions complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to a regulatory requirement or on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees, and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure."

1.1. Confidentiality of FinCEN SARs:

A FinCEN Suspicious Activity Report (FinCEN SAR), and any information that would reveal the existence of the FinCEN SAR (collectively, "FinCEN SAR information"), is confidential, and may not be disclosed except as specified in 31 U.S.C. 5318(g)(2) and in FinCEN's regulations (31 CFR Chapter X).

1.2. FinCEN SAR Sharing:

FinCEN, the Federal Banking Regulators, the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC) have concluded that any depository institution, broker-dealer in securities, futures commission merchant, and introducing broker in commodities may share the FinCEN SAR, or any information that would reveal the existence of the FinCEN SAR, with its head office or parent entity (whether domestic or foreign). (See "Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies," January 20, 2006 and "Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities," January 20, 2006.)

In addition, any depository institution, broker-dealer in securities, futures commission merchant, introducing broker in commodities, or casino that has filed a FinCEN SAR may share the FinCEN SAR, or any information that would reveal the existence of the FinCEN SAR, with an affiliate, as defined in FinCEN guidance (respectively, FIN-2010-G006 "Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates," Nov. 23, 2010; FIN-2010- G005, "Sharing Suspicious Activity Reports by Securities Broker-Dealers, Mutual Funds, Futures Commission Merchants, and Introducing Brokers in Commodities with Certain U.S. Affiliates;" FIN-2017-G001, "Sharing Suspicious Activity Reports with U.S. Parents and Affiliates of Casinos," January 4, 2017), provided the affiliate is subject to a FinCEN SAR regulation. The sharing of FinCEN SARs with head offices and affiliates facilitates the identification of suspicious transactions taking place through the depository institution's affiliates that are subject to a FinCEN SAR rule. Therefore, such sharing within the depository institution's corporate organizational structure is consistent with the purposes of Title II of the BSA.

1.3. Prohibition on Disclosures by Financial Institutions:

Federal law (31 U.S.C. 5318(g)(2)) provides that a financial institution, and its directors, officers, employees, and agents who, pursuant to any statutory or regulatory authority or on a voluntary basis, report suspicious transactions to the government, may not notify any person involved in the transaction that the transaction has been reported. Provided that no person involved in the suspicious activity is notified, 31 CFR Chapter X clarifies that the following activity does not constitute a prohibited disclosure:

- Disclosure of FinCEN SAR information to certain governmental authorities or other examining authorities that are otherwise entitled by law to receive FinCEN SAR information or to examine for or investigate suspicious activity;
- Disclosure of the underlying facts, transactions, and documents upon which a FinCEN SAR is based; and
- For those institutions regulated by a federal functional regulator (federal bank regulatory agencies,

© gettechnical inc 2021

the SEC, and the CFTC), the sharing of FinCEN SAR information within an institution's corporate organizational

structure, for purposes that are consistent with the Bank Secrecy Act, as determined by regulation or guidance.

1.4. Prohibition on Disclosures by Government Authorities:

Federal law (31 U.S.C. 5318(g)(2)) also provides that an officer or employee of any Federal, state, local, tribal, or territorial government within the United States who has knowledge that such report was made, may not disclose to any person involved in the transaction that the transaction has been reported, other than as necessary to fulfill the official duties of such officer of employee. FinCEN's regulations clarify that "official duties" must be consistent with Title II of the Bank Secrecy Act and shall not include the disclosure of a FinCEN SAR, or any information that would reveal the existence of a FinCEN SAR, in response to a request for disclosure of non-public information or a request for use in a private legal proceeding, including a request pursuant to 31 CFR § 1.11.

1.5. FinCEN SAR Filing Instructions:

1. **Who Must File:** Certain financial intuitions operating in the United States shall file with FinCEN, to the extent and in the manner required by 31 CFR Chapter X and 12 CFR §§ 21.11, 163.180, 208.62, 353.3, and 748.1, a report of any suspicious transaction relevant to a possible violation of law or regulation. The following financial institutions are required to file a FinCEN SAR: Banks (31 CFR §1020.320) including Bank and Financial Holding Companies (12 CFR § 225.4); Casinos and Card Clubs (31 CFR § 1021.320); Money Services Businesses (31 CFR § 1022.320); Brokers or Dealers in Securities (31 CFR § 1023.320); Mutual Funds (31 CFR § 1024.320); Insurance Companies (31 CFR § 1025.320); Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR § 1026.320); Residential Mortgage Lenders and Originators (31 CFR § 1029.320), and Housing Government Sponsored Enterprises
(31 CFR § 1030.320).

2. **Filing Deadlines:** A FinCEN SAR shall be filed no later than 30 calendar days after the date of the initial detection by the reporting financial institution of facts that may constitute a basis for filing a report. If no suspect is identified on the date of such initial detection, a financial institution may delay filing a FinCEN SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the financial institution shall immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a FinCEN SAR. Financial institutions wishing voluntarily to report suspicious transactions that may relate to terrorist activity may call FinCEN's Financial Institutions Hotline at 1-866- 556-3974 in addition to filing timely a FinCEN SAR.

3. **Filing Requirements for Financial Institutions:** A financial institution must report any transaction that requires reporting under the terms of 31 CFR Chapter X if the transaction is conducted or attempted by, at, or through the financial institution and involves or aggregates at least $5,000 ($2,000 for money services businesses, except as provided in Section 6 of this document) and the financial institution knows, suspects, or has reason to suspect that the transaction or pattern of transactions of which the transaction is a part:

- Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
- Is designed, whether through structuring or other means, to evade any requirement of 31 CFR Chapter X or any other regulation promulgated under the Bank Secrecy Act, Public Law 91-508, as amended, codified at 12 U.S.C 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5332.
- Has no business or apparent lawful purpose or is not the sort in which the particular customer

© gettechnical inc 2021

would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or
- Involves the use of the financial institution to facilitate criminal activity.

4. Additional Filing Instructions for Banks: In addition to the above requirements, a bank (as defined in 31 CFR § 1010.100) must file a FinCEN SAR for activity (as required by 31 CFR § 1020.320 and 12 CFR §§ 21.11, 163.180, 208.62, 353.3, and 748.1) involving:

- **Insider abuse involving any amount.** Whenever the bank detects any known or suspected Federal criminal violations, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying one of its directors, officers, employees, agents or other institution- affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.
- **Violations aggregating $5,000 or more where a suspect can be identified.** Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $5,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an "alias," then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported.
- **Violations aggregating $25,000 or more regardless of a potential suspect.** Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $25,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

5. Voluntary FinCEN SAR Filings: Financial institutions may also file with FinCEN a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR Chapter X. A voluntary filing does not relieve a financial institution from the responsibility of complying with any other reporting requirements imposed by the SEC, the CFTC, a self-regulatory organization (SRO) (as defined in section 3(a)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78c (a)(26)), or any Registered Futures Association (RFA) or Registered Entity (RE) (as these terms are defined in the Commodity Exchange Act, 7 U.S.C. 21 and 7 U.S.C. 1a(29)).

6. Exceptions: The following are exceptions to the FinCEN SAR reporting requirements:

- A bank, casino, broker or dealer in securities (BD), futures commission merchant (FCM), or introducing broker in commodities (IB-C) is not required to file a FinCEN SAR for a robbery or burglary committed or attempted against the financial institution when the robbery or burglary is reported to appropriate law enforcement authorities.
- A FinCEN SAR is not required to be filed for lost, missing, counterfeit, or stolen securities that are reported pursuant to the requirements of 17 CFR § 240.17f-1.
- A BD is not required to file a FinCEN SAR on violations of any of the Federal securities laws or the rules of a SRO by the BD or any of its officers, directors, employees or other registered representatives, other than a violation of 17 CFR § 240.17a-8 or 17 CFR § 405.4, so long as such

© gettechnical inc 2021

violation is appropriately reported to the SEC or an SRO.

- An FCM or an IB-C, or any of its officers, directors, employees or associated persons, is not required to file a FinCEN SAR for a violation of the Commodity Exchange Act (7 U.S.C. 1 et seq.), the regulations of the CFTC (17 CFR Chapter 1), or the rules of any RFA or RE (as those terms are defined in the Commodity Exchange Act, 7 U.S.C. 21 and 7 U.S.C. 1a(29)), as long as such violation is appropriately reported to the CFTC, an RFA, or RE. This exception does not apply to violations of 17 CFR § 42.2.
- An insurance company is not required to report the submission to it of false or fraudulent information to obtain a policy or make a claim, unless the company has reason to believe that that the false or fraudulent submission relates to money laundering or terrorist financing.
- An issuer of money orders or traveler's checks is not required to report a transaction or pattern of transactions when the transactions were identified through a review of clearance records or other similar records and the transaction amount or aggregated transaction amount involves funds or other assets of less than $5,000.

7. Additional Reporting: The Bank Secrecy Act requires financial institutions to file a Currency Transaction Report (CTR) in accordance with the Department of the Treasury's implementing regulations (31 CFR § 1010.310) whenever a currency transaction exceeds $10,000. If a currency transaction exceeds $10,000 and is otherwise reportable as suspicious activity, the institution must file both a CTR (reporting the currency transaction) and a FinCEN SAR (reporting the suspicious activity). If a currency transaction is $10,000 or less and is otherwise reportable as a suspicious activity, the institution should only file a FinCEN SAR. Appropriate records must be maintained in each case. Residential Mortgage Lenders and Originators are required to file Form 8300, Report of Cash Payments Over $10,000 Received in a Trade or Business, instead of a CTR.

1.6. FinCEN SAR Electronic Filing Instructions

1.6.1. General Instructions:

1. **Filing Reports:** This report must be E-filed through the Financial Crime Enforcement Network (FinCEN) BSA E-Filing System. Go to http://bsaefiling.fincen.treas.gov to register if not already registered. Financial institutions that file reports individually will use FinCEN's discrete FinCEN SAR to file their reports. Financial institutions that use batch filing or system-to-system filing to transmit multiple reports must transmit files that conform to the requirements of FinCEN's "General Specifications for Electronic Filing in XML format of Bank Secrecy Act (BSA) Reports" (General Specifications) and "FinCEN Suspicious Activity Report (FinCEN SAR) XML Filing Requirements."

2. **Recording Information:** Complete each FinCEN SAR by providing as much information as possible. Although all items should be completed fully and accurately, items marked with an asterisk (*) must be completed even when the required data are unknown. Filers must follow the electronic filing instructions for these items by providing the required data or, if instructions permit, by checking the box "Unknown" to indicate that the required data was unknown. Items that do not begin with an asterisk must be completed if the data are known and will be left blank if the data are unknown. If an item's instructions differ from the General Instructions the item's instructions must be followed. These instructions supersede all prior FinCEN SAR instructions and FinCEN guidance on use of special responses in FinCEN SAR items when the data are unknown or not available in an electronic filing. Therefore, the use of special responses such as "UNKNOWN," "NONE," "NOT APPLICABLE," or "XX" and their variants is prohibited in the FinCEN SAR.

   NOTE: Throughout these instructions the phrases "check box" and "select option" or similar wording is used to denote checking an appropriate box or selecting a drop-down list option in certain data items on the discrete FinCEN SAR. These are deemed equivalent to instructions in the XML Filing Requirements to enter appropriate codes or responses in the same data items in XML-format transmission files. For example, the requirement to check box 1 "Initial report" in the discrete FinCEN SAR is the equivalent of entering "Y" in XML element <InitialReportIndicator>.

© gettechnical inc 2021

NOTE: Throughout these instructions there are requirements to complete items multiple times in a discrete FinCEN SAR if the filer has multiple entries for that item. This is deemed equivalent to completing multiple XML elements for that item in the XML Filing Requirements. For example, these instructions direct filers to complete multiple Item 6 "Alternate name" fields if the filer has knowledge of multiple alternate names for a subject. This is equivalent to a batch filer recording multiple XML <PartyName> elements and appropriate sub-elements for the same subject.

3. **Corrected/Amended Reports:** A corrected report on a previously-filed FinCEN SAR or prior FinCEN SAR version must be filed whenever errors are discovered in the data reported in that FinCEN SAR. An amended report must be filed on a previously-filed FinCEN SAR or prior FinCEN SAR versions whenever new data about a reported suspicious activity is discovered and circumstances will not justify filing a continuing report (see General Instruction 4). Both corrected and amended reports must be completed in their entirety, with the necessary corrections or amendments made to the data. In both cases box 1b "Correct/Amend prior report" must be checked. If known, the prior report's BSA Identifier (BSA ID) must be entered in field 1e. If the prior report's BSA ID is unknown, field 1e should be zero-filled. All corrections or amendments must be described completely at the beginning of the Part V Suspicious Activity Information – Narrative section. If a FinCEN SAR is filed to correct or amend a prior FinCEN SAR version, the FinCEN SAR must be completed in its entirety. This includes FinCEN SAR items that apply to the suspicious activity but were not present on the prior FinCEN SAR version. FinCEN SAR items not on the prior FinCEN SAR version need not be described in the narrative. BSA IDs are provided in acknowledgement records sent to member financial institutions by the BSA E-Filing System.

4. **Continuing Reports:** A continuing report should be filed on suspicious activity that continues after an initial FinCEN SAR is filed. Continuing reports should be filed at least every 90 days until the suspicious activity ceases. Continuing reports must be completed in their entirety, including the information about all subjects involved in the suspicious activity and all financial institutions where the activity occurred. The continuing report Part V narrative should include all details of the suspicious activity for the 90-day period encompassed by the report, and only such data from prior reports as is necessary to understand the activity. Do not reproduce the narratives from prior reports in the continuing report. Provide both the dollar amount involved in the suspicious activity for the 90-day period in Item 28 and the cumulative dollar amount for the current and all prior related reports in Item 31. If continuing losses are involved for any financial institution recorded in Part III, record the 90-day loss in Item 67 and the cumulative loss in Part V.

5. **Joint Report:** A FinCEN SAR may be jointly filed when two or more distinct financial institutions recorded in Part III "Information about Financial Institution Where Activity Occurred" collaborate in filing a single FinCEN SAR on suspicious activity involving all of the collaborating financial institutions. Financial institutions are "distinct" for this purpose when they are different legal entities; a financial institution is not distinct from its own branches. Joint filing of a single FinCEN SAR is prohibited when any of the Part I "Subject Information" subjects of the would-be jointly filed FinCEN SAR have a box in Item 24 checked that identifies the subject as a director, employee, officer, or owner/controlling shareholder of the filing institution or a would-be joint filer. In that case separate FinCEN SARs must be filed by each institution. To be a jointly-filed FinCEN SAR, box 1d "Joint report" must be checked. In addition, the filing institution listed in Part IV "Filing Institution Contact Information" must identify in Part V "Suspicious Activity Information – Narrative" which Part III "Information about Financial Institution Where Activity Occurred" institutions are joint filers. The filing institution must include joint filer contact information in Part V, along with a description of the information provided by each joint filer. Record joint filer information in Part III Items 51 through 65 and joint filer branch information in Part III Items 68 through 74. Filing a joint FinCEN SAR does not relieve joint filers of the responsibility to report information about the suspicious activity that was not included in the joint filing. A filing institution cannot designate another institution as a joint filer unless the designated joint filer is aware of and approves the FinCEN SAR filing in its entirety. A filer that designates another institution as a joint filer without gaining that institution's agreement to the joint filing and

© gettechnical inc 2021

approval of the contents of the joint filing may have committed a willful violation of the Bank Secrecy Act, if the improper designation leads to the disclosure of the FinCEN SAR filing to a person not entitled to information about the filing. Both filers and joint filers are required to keep copies of the FinCEN SAR and their own supporting documentation for five (5) years after the date of filing.

6. **Supporting Documentation:** Filers can include a single Microsoft Excel compatible comma separated values (CSV) file with no more than one megabyte of data as an attachment to the FinCEN SAR. The contents of this file must be described in Part V. This file would be most suitable for documenting transaction records that are too numerous to record in Part V. Do not include any other supporting documentation with the FinCEN SAR. Instead, describe in Part V other supporting documentation not included in the file. Filers must retain all supporting documentation or a business record equivalent for five (5) years from the date of the report (31 CFR § 1010.430). All supporting documentation (such as copies of instruments; receipts; sale, transaction or clearing records; photographs; and surveillance audio or video recordings) must be made available to appropriate authorities upon request. See Attachment D for information on attaching comma separated (.CSV) files to a FinCEN SAR filing.

7. **Addresses:** For addresses in the U.S., Canada, or Mexico enter the permanent street address, city, two or three letter state/territory/province code, ZIP Code or foreign postal code, and two-letter country code or U.S. Territory code for the individual or entity recorded in Part I, Part III, or Part IV. Provide the apartment number or suite number, if known, following the street address. A non-location address such as a post office box or rural route number should be used only if no other street address information is available. ZIP Codes must be five or nine digits. ZIP Codes and foreign postal codes must be entered without formatting or special characters such as spaces or hyphens. For example, the ZIP Code 12345-6120 would be entered as 123456120. The foreign postal code HKW 702 would be entered HKW702. When an address is in a U.S. Territory the territory code must be entered in the state and country fields. For other foreign addresses enter the street address, city, postal code, and two letter country code or address equivalents. Leave the state item blank, including the "Unknown box" when provided. If a foreign address contains address information that does not conform to the FinCEN SAR address format, record equivalent address information in the FinCEN SAR address items (except state) and ignore non-conforming data. The complete foreign address should be recorded in the FinCEN SAR's Part V narrative section. Complete any address item that is known, even if the entire address is not known. No abbreviations are permitted in city names, which must be completely spelled out. A U.S. city name must match the city name used by the U.S. Postal Service for the associated state and ZIP Code. U.S. State and Territory codes must conform to the codes used by the United States Postal Service as documented in ISO 3166-2:US. Canadian province and territory codes must conform to the codes used by the Canadian Post Corporation as documented in ISO 3166-2:CA. Mexican state and federal district codes must conform to ISO 3166-2:MX. Country codes and U.S. Territory Codes must conform to the codes documented in ISO 3166-2. The ISO lists are available through the International Standards Organization.

8. **Telephone Numbers:** Record all telephone numbers, both foreign and domestic, as a single number string without formatting or special characters such as parentheses or hyphens. For example, a number in the format (NNN) NNN-NNNN would be recorded as NNNNNNNNNN. Indicate the type of telephone number provided (home, work, mobile, or fax) by checking the appropriate box. Provide the telephone extension number if known. Telephone numbers that are part of the North American Numbering Plan used by the U.S., Canada, many Caribbean countries, and current/former U.S. Pacific island protectorates must consist of an area code and seven-digit telephone number. Other foreign telephone numbers should include the country number code. If only a partial telephone number is known record that number in the phone number item and explain in Part V that the entry is a partial number.

9. **Identifying Numbers:** Enter all identifying numbers as a single text string without formatting or special characters such as hyphens or periods. An identifying number in the format NNN-NN-NNNN would be entered as NNNNNNNNN. Such numbers include account numbers, alien

© gettechnical inc 2021

registration numbers, CRD, CUSIP®, driver's license numbers, state identifications, EINs, IARDs ITINs, passport numbers, RSSDs, SEC IDs, and SSNs.

10. **Monetary Amounts:** Record all monetary amounts in U.S. Dollars rounded up to the next whole dollar. The amount $5,265.25 would be rounded up to $5,266. If the amount involves a foreign currency, record the currency name, amount, and country of origin in Part V. When converting a foreign currency to U.S. Dollars use an exchange rate for the date or dates the foreign currency was involved in the suspicious activity.

11. **Prohibited Words and Phrases:** Do not use the following words or variations of these words in text fields, other than in Part V:
    a. AKA
    b. COMPUTER GENERATED
    c. CUSTOMER
    d. DBA
    e. NON CUSTOMER
    f. NONE
    g. NOT APPLICABLE
    h. OTHER
    i. SAME
    j. SAME AS ABOVE
    k. SEE ABOVE
    l. SEE NARRATIVE
    m. SIGNATURE CARD
    n. T/A
    o. UNKNOWN
    p. VARIOUS
    q. XX

12. **Name Editing Instructions:** Because many names do not consist of a single first name, middle name, and last name, care must be taken to ensure these names are entered properly in the BSA FinCEN SAR. This is especially important when there are separate fields for the last name, first name, and middle name. Some names have multiple surnames (family names) or multiple given names that do not include a middle name. Others may not be written in [first name] [middle name] [last name] order. Multiple surnames must be entered in the last name field. For example, Hispanic names may be written in the order of given name, father's last name, and mother's last name, e.g., "Juan Vega Santiago." Thus the surname "VEGA SANTIAGO" would be entered in the last name field with "JUAN" entered in the first name field. Some Hispanic surnames consist of three names (e.g., father's last name, mother's last name, and husband's father's last name in the case of a married woman). In that case all three would be entered in a last name field. Hispanic names do not have middle names, so a multiple Hispanic given name such as "Rosa Maria" would be recorded in the first name field. In some cultures names consist of multiple first names and a single family name, not necessarily in (first name) (last name) order. For example, the Korean name "Kim, Chun Nam" consists of the family name "Kim" and the first name "Chun Nam" separated by a comma and space. There is no middle name. In this case "KIM" would be entered in the last name field and "CHUN NAM" would be entered in the first name field. Nothing is entered in the middle name field. When an individual name is entered in a single name field it should be entered in [first name] [middle name] [last name order regardless of any foreign naming conventions. Thus, "Kim, Chun Nam" would be entered as "CHUN NAM KIM" in a single name field. Punctuation and special characters should be used in names only when they are part of the name. For example, the period in "Expedia.Com" should be included because it is part of the name. Entry of middle initials is permitted when a middle name is unknown. Do not include a period after a middle initial when the initial represents a name abbreviation. Abbreviations in names are prohibited unless an abbreviation is part of a legal name or the name is unknown. A name suffix may be abbreviated, i.e. Junior can be JR, Senior can be SR, the Third can be III, etc.

13. **Reporting Cyber Events:** Cyber events directly affecting the financial institution or the financial

© gettechnical inc 2021

institution's customer are occurring on an ever-increasing basis. Since the implementation of the new FinCEN SAR in 2011, a significant number of FinCEN SARs have been filed to record the events with the data being recorded in Part V, the FinCEN SAR Narrative. The data collected and submitted has provided law enforcement with valuable leads and insight into this emerging field. A review of the data reported indicates that prompt retrieval of cyber event information is a critical step in combating malicious cyber activity. To facilitate and support prompt identification and retrieval of malicious cyber event information, specific cyber fields (42, 43, and 44) have been added to Part II, the Suspicious Activity Information section of the FinCEN SAR. These fields are not meant to be exhaustive or to replace attachments. Use of these fields to highlight selected information (that may also be in attachments) can assist law enforcement in identifying key indicators. Due to the growing prevalence and technological sophistication of cyber-enabled financial crime, FinCEN encourages financial institutions to develop a basic understanding of what comprises a cyber event. Being familiar with selected key vocabulary is essential in describing these cyber events to law enforcement. Completion of cyber event fields 42 to 44 is not mandatory, but is encouraged where financial institutions have sufficient capacity to do so. While use of the fields may not be mandatory, filing on certain cyber events and cyber-enabled financial crime may be mandatory under existing filing requirements—see FinCEN Advisory FIN-2016-A005 for more information.

A principal source of cyber related information will be the financial institutions' internal technology department or external technology contractor. FinCEN recognizes that institutions have varying familiarity with and access to cyber-related information in their compliance departments and therefore encourages the involvement of available IT resources on an ongoing basis. Financial institutions should review established internal departmental protocols to ensure prompt review and reporting of cyber event information. Reporting cyber event information is not a new requirement and financial institutions are expected to report this information when available. To assist institutions in identifying when to use the new cyber fields, FinCEN is providing the examples below. Please note that these examples highlight instances where an institution may be limited in its ability to identify cyber-related information due to limits in cyber expertise or resource availability. Each example is an acceptable and appropriate use of these fields.

Example 1.
Bank A is told by its customer, ABC Corp, that a recent wire payment issued from its account was fraudulent. Bank A is told that fraudsters imitated the CEO of ABC Corp.'s e-mail to instruct ABC employees to wire funds from ABC's accounts at Bank A to an account at Bank B. ABC Corp tells Bank A that these fraudulent e- mails were made to look like the CEO used the e-mail address CEO@ABCcorp.co instead of the legitimate CEO@ABCcorp.com. These fraudulent e-mails appeared to be instructing employees to issue urgent payments to one of ABC's suppliers for $300,000. Bank A recognizes this as a Business E-mail Compromise (BEC) scheme. In the FinCEN SAR narrative, Bank A describes the incident and mentions the term "BEC Fraud" and FinCEN advisory FIN-2016-A003.

Bank A places the following information in the new fixed fields on the FinCEN SAR form:

Item 42: Cyber Event

b. Against Financial Institution Customer(s) [check box]

Field 44f. Suspicious e-mail address

44f1. Event value: CEO@ABCcorp.com

Example 2.

Bank A is told by its customer, ABC Corp, that a recent wire payment issued from its account was fraudulent. Bank A is told by its customer that the CEO of ABC Corp.'s e-mail was hacked and used to instruct ABC employees to wire funds from ABC's accounts at Bank A to an account at

© gettechnical inc 2021

Bank B. ABC Corp tells Bank A that these e-mails were made to look like the CEO was instructing employees to issue payments to ABC's suppliers for $300,000. No additional technical information was provided to Bank A. Bank A recognizes this as a Business E-mail Compromise (BEC) scheme. In the FinCEN SAR narrative, Bank A describes the incident and mentions the term "BEC Fraud" and FinCEN advisory FIN-2016-A003.

Bank A places the following information in the new fixed fields on the FinCEN SAR form:

Item 42: Cyber Event

b. Against Financial Institution Customer(s) [check box] Item 44: BLANK

Example 3.

Bank C identifies a cyber incident that targeted Bank C's own systems, resulting in access to Bank C's payment systems and an attempted transfer of $1 million through Bank C's 123-wire system. Bank C's compliance team asks its IT department for additional technical information related to this incident, and whether there were any key indicators associated with the event. The IT department is still gathering information, but has identified one piece of relevant malware and the IP address that relayed instructions to attempt the $1 million funds transfer. They also have a .csv file containing possibly related technical information that Bank C decides to include as an attachment.

Bank C files a FinCEN SAR with the following information in the new fixed fields:

Item 42: Cyber Event

a. Against Financial Institution [check box]

Field 44a. Command & Control IP Address

44a1. Event value: 127.0.0.1

44a2. Date (2017/01/01)

44a3. UTC Time (00:00:01)

Field 44c. Malware MD5, Malware SHA-1, Malware SHA-256:

44c1Event value: 9e107d9d372bb6826bd81d3542a419d6

Field 44j. Targeted System:

44j1. Event value: 123-wire

Example 4.

Bank D identifies an incident that targeted Bank D's own systems, resulting in access to Bank D's payment systems and an attempted transfer of $50,000 through Bank D's 123-wire system. Bank D's compliance team asks its IT department for additional technical information related to this incident, and whether there were any key indicators associated with the event. Bank D's IT department confirms that the incident was a cyber event against Bank D, but is unable to spend resources locating additional information due to their necessary focus on continuity of business operations. Bank D files a FinCEN SAR based on the available information.

Bank D files a FinCEN SAR with the following information in the fixed fields:

Item 42: Cyber Event

a. Against Financial Institution [check box]

Field 44j. Targeted System:

44j1. Event Indicator value: 123-wire

Example 5.

© gettechnical inc 2021

Bank E is told by its customer that a fraudulent wire was sent from their online banking account. The customer does not know how fraudsters gained access to their account. Bank D is able to identify the record of the fraudulent wire and when it occurred. Bank D's compliance department asks its IT department for IP log information associated with the targeted customer's account at the time of the fraudulent wire transfer. The IT department is able to provide the information from their logs.

Bank E files a FinCEN SAR with the following information in the new fixed fields:

Item 43:

a. IP address: 127.0.0.1 b. Date: 2017-01-30
c. UTC Time: 00:00:01

1.6.2. Item Instructions:

NOTE: Critical fields are identified with the * symbol in front of the data element number.

---------- Type of Filing ----------

*1. Type of filing (check all that apply)

a. Initial report
b. Correct/Amend prior report
c. Continuing activity report
d. Joint report
e. Prior report BSA Identification Number if items 1b or 1c are checked

Item *1 Type of filing: Check box 1a "Initial report" if this is the first report filed on the suspicious activity. Check box 1b "Correct/Amend prior report" if the report corrects or amends a previously-filed FinCEN SAR. See General Instruction 3 for additional instructions on filing corrected or amended SARs. Check box 1c "Continuing activity report" if the FinCEN SAR continues reporting on previously-reported suspicious activity. If the FinCEN SAR corrects a previously-filed continuing activity report, both 1b and 1c must be checked. See General Instruction 4 for additional instructions on filing continuing activity reports. Check box 1d "Joint report" if a FinCEN SAR of any filing type is filed jointly by two or more financial institutions. See General Instruction 5 for additional instructions on filing joint reports. If box 1b or 1c is checked, the prior report's BSA Identifier (BSA ID) must be recorded in field 1e. Enter 14 zeros if the prior report BSA ID is unknown.

2. Filing Institution Note to FinCEN

Item 2, Filing Institution Note to FinCEN: This 50 character field is provided for

the filer to alert FinCEN that this FinCEN SAR is being filed in response to a current specific geographic targeting order (GTO) or advisory or other activity. If completing for a GTO or advisory enter the GTO or advisory title/reference. Provide a brief description of the other activity. Leave Item 2 blank if the FinCEN SAR does not relate to a GTO, advisory, or other targeted activity.

---------- Part I Subject Information ----------

Part I Subject Information: Complete a Part I section on each known subject involved in the suspicious activity. Persons who are victims of the suspicious activity are not subjects and should not be recorded in a Part I section. Victim information, if necessary for a complete description of the suspicious activity, should be recorded in Part V. If the subject is or all subjects are unknown, complete a single Part I record with box 2b checked to show that all subject information was unavailable for critical Items 4, 5, 11, 12, 13, 14, 15, 17, and 18. These critical items (denoted with an asterisk "*") except Item 24 must be blank. Record the nature of the unknown subject(s) in Part V. If the suspicious activity involves known and unknown subjects, complete a Part I section on each known subject and record the nature of the unknown subject(s) in Part V. Do not complete Part I records on the unknown subjects when there are known subjects.

3. Check:

© gettechnical inc 2021

a. If entity
b. If all critical* subject information is unavailable (does not include item *25)

Item 3a Check if entity: Check box 3a if the person described in Part I is an entity and not an individual. Item 3b Check if all critical subject information is unavailable: Check box 3b if the information in Part I is unavailable for all critical subject items except Item 25. These critical items (4, 5, 11, 12, 13, 14, 15, 17, and 18) and their associated "Unknown" fields must be left blank.

* 4. Individual's last name or entity's legal name

a. (check if) unknown

Item *4 Individual's last name or entity's legal name: Enter the individual's last name or the entity's legal name. The legal name is the name on the articles of incorporation or other document that established the entity. Do not abbreviate names unless an abbreviation is part of the legal name. Item 4 and box 4a "Unknown" must be blank if box 3b is checked. Leave item 4 blank and check box 4a "Unknown" if the individual's last name or the entity's legal name is unknown and box 3b is not checked.

* 5. First name

a. (check if) unknown

Item *5 First name: Enter the individual's first name. If the first name is unknown leave item 5 blank and check box 5a "Unknown." Leave Item 5 and box 5a "Unknown" blank if box 3a or 3b is checked.

6. Middle name

Item 6 Middle name/initial: Enter the individual's middle name or initial. Leave this item blank if the middle name or initial is unknown or box 3a is checked.

7. Suffix

Item 7 Suffix name: Enter the individual's suffix such as JR, SR, III, etc. Leave this item blank if the suffix is unknown or the individual's legal name does not include a suffix.

8. Gender
a. Male
b. Female
c. Unknown

Item 8 Gender: Select options 8a Male or 8b Female if individual's gender is known. Select option 8c "Unknown" if the individual's gender is unknown. Leave Item 8 blank if the subject is an entity. Item 8 (Gender) does not create an obligation for a financial institution to collect this data when such collection would be in conflict with the financial institution's obligations under any other federal law.

9. Alternate name, e.g., AKA if individual; DBA/ trade name if entity.

Item 9 Alternate name: Enter the individual's also known as (AKA) name or the entity's doing business as (DBA) name if different from the name entered in Items 4-6. Do not include the acronyms AKA or DBA with the name. Multiple Item 9 fields may be completed if multiple subject alternate names are known.

10. Occupation or type of business

a. NAICS Code

Item 10 Occupation or type of business: Record the occupation, profession, or type of business of the individual or entity recorded in Part I. Use specific descriptions such as doctor, carpenter, attorney, used car dealership, plumber, truck driver, hardware store, etc. Do not use non- descriptive items such as businessman, merchant, retailer, retired, or self-employed. If words like self-employed, unemployed, or retired are used, add the current or former profession if known (e.g. self-employed building contractor,

© gettechnical inc 2021

retired teacher, or unemployed carpenter). If the occupation or business activity can be described in more detail, include the additional information in Part V.

Item 10a NAICS Code: select the North American Industry Classification System (NAICS) code for the occupation or type of business entered in Item 10. Batch filers should only enter codes from the list of NAICS Codes authorized for use in the FinCEN SAR and located on the BSA E- Filing Web Site (http://bsaefiling.fincen.treas.gov/main.html) or from the U.S. Census Bureau NAICS list at https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2017. If the Census Bureau list is used filers cannot substitute a sector code (such as 11 Agriculture, Forestry, Fishing and Hunting) for an actual three to six number NAICS Code (such as 11114 Wheat Farming).

Items *11 - *14 Subject address items: Enter the subject's permanent street address, city, two or three letter state/territory/province code (U.S./Canada/Mexico only), ZIP Code or foreign postal code, and two letter country or

U.S. Territory code. Complete any address item that is known, even if the complete address is unknown. If an address item is unknown, leave that item blank and check box 11a "Unknown." If box 3b is checked all address items and check boxes must be blank. See General Instruction 7 for additional information on entering addresses. Multiple sets of address fields may be completed if multiple present and past subject addresses are known.

*11. Address

a. (check if) unknown

*12. City

a. (check if) unknown

13. State

a. (check if) unknown

*14. ZIP/Postal Code

a. (check if) unknown

*15. Country Code

a. (check if) unknown

*16. TIN (enter number in space provided and check appropriate type below)

b. (check if) unknown

Item *16 TIN: Enter the subject's U.S. taxpayer identification number (TIN) or foreign equivalent without formatting or punctuation. If the number is unknown, check box 16a "Unknown" and leave Item 16 blank. Leave item 16 and box 16a “Unknown” blank if box 3b is checked. See General Instruction 9 for information on entering identifying numbers.

17. TIN type

a. EIN
b. SSN-ITIN
c. Foreign

Item 17 TIN type: Identify the type of TIN recorded in Item 16. Select option 17a “EIN” if the subject has a U.S. Employer Identification Number (EIN). Box 3a “If entity” must be checked because an EIN is assigned only to an entity. Select option 17b “SSN-ITIN” if the subject has a U.S. Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN). Select option 17c “Foreign” if the subject has a foreign TIN of any type. Box 3a must be checked if the foreign subject is an entity. If 17c is checked, record in Part V the name of the country that issued the foreign TIN. Enter the subject’s TIN type if known even if the actual TIN is unknown and Item 16a “Unknown” is checked. If a 9-digit TIN is entered in Item 17 but the TIN type is unknown, select option 17a “EIN” if the subject is an entity and

© gettechnical inc 2021

option 17b “SSN-ITIN” if the subject is an individual. TINs that are not 9 digits are presumed to be foreign, so option 17c “Foreign” would be selected.

* 18. Form of identification for subject:

a. (check if) unknown
b. Driver’s license/state ID
c. Passport
d. Alien registration
e. Number
f. Issuing State
g. Country
z. Other (and specify type in space provided)

Item *18 Form of identification: Enter in Item 18 the information used to identify the individual or entity. Select option 18b if the identification was a driver's license or state ID, 18c if the identification was a passport or 18d if the identification was an alien registration. Select option 18z if a different identification was provided and describe that identification in the "Other" text field. “Other” identification could include such things as an entity’s business license or incorporation documents, corporate ID cards, local government ID cards, etc. Enter the identification number in field 18e "Number." Do not include formatting such as hyphens or periods. Select the appropriate state option in field 18f "Issuing state" if the identification issuer was a U.S., Canadian, or Mexican state, territory, or province. Select the appropriate country option in field 18f "Country" if the issuer was a country. If field 18f “Issuing state” contains an entry, then 18g “Country” must contain “US,” “CA,” or “MX” as appropriate. Enter the data on the country that issued the ID or where the ID was issued. See General Instruction 7 for information about the codes to enter in state and country items. If the identification issuer does not have a code, select the option for the issuer's country in field 18g. For example, if the issuer was the London Police Department United Kingdom would be selected in 18g. Record the name and nature of the issuer in Part V. Enter all identification data that is available. Check box 18a “Unknown” only if all identification information is unknown but the subject is known. Leave all fields in Item 18 blank if box 3b has been checked. Multiple sets of Item 18 fields may be completed if multiple types of identification for a subject are known. See General Instruction 9 for information on entering identifying numbers.

* 19. Date of birth MM/DD/YYYY

a. (check if) unknown

Item *19 Date of birth: If the subject is an individual enter the subject's data of birth in Item 19. Filers of FinCEN’s discrete FinCEN SAR must use the format MM/DD/MMYY where MM = month, DD = day, and YYYY = year. Batch filers must use the format YYYYMMDD. If the birth day and or month is unknown, enter “00” for the unknown day or month. For example, a date of birth with an unknown day in February 1978 would be entered as 02/00/1978 in a discrete FinCEN SAR and 19780200 in a batch filed FinCEN SAR. Do not enter zeros for the year if the year is unknown. If the year of birth or the complete date of birth is unknown, check box 19a "Unknown" and leave Item 19 blank. If box 3a or b is checked, Item 19 and box 19a “Unknown” must be blank.

20. Phone number – type

a. Home
b. Work
c. Mobile
d. Fax

Item 20 Phone number – type: selected the telephone number type that applies to the telephone number recorded in Item “21. Phone Number.” If a number is known but the type is unknown leave Item 20 blank. If a number is known but the type is unknown, select option “a. Home” if the subject is an

© gettechnical inc 2021

individual and “b. Work” if the subject is an entity. Multiple sets of Item 20, Item 21, and Item 21a fields may be completed if multiple telephone numbers for the subject are known

21. Phone number

a. Extension (if any)

Item 21 Phone number: Enter the subject's U.S. or foreign telephone number with no formatting such as parentheses, spaces, or hyphens. If the telephone number is unknown, leave item 21 blank. See General Instruction 8 for information on entering telephone numbers. Multiple sets of Item 21 and Item 21a fields may be completed if multiple telephone numbers for the subject are known.

Item 21a Ext. (if any): Enter the telephone extension associated with the subject's telephone number. Leave Item 21a blank if there is no extension or the extension is unknown.

22. E-mail address (if available)

Item 22 E-mail address: Enter the subject's e-mail address if known. Include all formatting, punctuation, and special characters in the e-mail address. Leave Item 22 blank if the e-mail address is unknown. If additional e-mail addresses are known for a subject, complete additional Item 22 fields. An e-mail address must contain the “@” sign and a period in the text following the “@” sign. Examples: johndoe@business.com or richardroephd@college.edu.

22a. Website (URL) address (if available)

Item 22a Website (URL) address: Enter the subject's website URL (Uniform Resource Locator) known. Include all punctuation and special characters present in the URL. If additional URLs are known for a subject, complete an additional Item 22a for each URL. Leave Item 22a blank if the URL is unknown.

23. Corroborative statement to filer?

a. Yes
b. No

Item 23 Corroborative statement: Select "Yes" if the subject individual has made a statement to the filer admitting to involvement in or otherwise substantiating the suspicious activity. Record in Part V the nature of the corroborative statement and how it was recorded, i.e. written confession, verbal statement, etc. Select "No" if no corroborative statement was made to the filer. Leave Item 23 blank of the subject is an entity

24. Relationship of the subject to an institution listed in Part III or IV (check all that apply)

a. Institution TIN
b. Accountant
c. Agent
d. Appraiser
e. Attorney
f. Borrower
g. Customer
h. Director
i. Employee
j. No relationship to institution
k. Officer
l. Owner or Controlling Shareholder
z. Other (and specify type in space provided)

Item 24 Relationship of the subject to an institution: If the subject has a relationship with a financial institution or individual listed in Part III or Part IV, enter the financial institution's TIN from Items 55 or 81 in field 23a "Institution EIN." Select all options 24b through 24l (but not 24j no relationship) that describe the relationship. If the relationship is not covered by any of options 24b through 24l, select

© gettechnical inc 2021

option 24z "Other" and enter a brief description of the relationship in the "Other" text field. Avoid descriptions that are too general. For example, the entry "broker" should be made more specific by indicating the relationship was "real estate broker," "securities broker," or "mortgage broker." If necessary, describe the relationship more fully in Part V. If the subject has no relationship with any of the financial institutions in Part III or Part IV, record box 24j "No relationship to institution" once for all institutions and enter the Part IV filing institution's EIN in the Item 24 "Institution TIN" field. Do not record box 24j for the subject if a relationship exists with any institution, even when there is no relationship with other institutions." The FinCEN SAR cannot be a joint FinCEN SAR if any of the options 24h "Director," 24i "Employee," 24k "Officer," or 24l "Owner or Controlling Shareholder" have been selected. If the subject had a relationship with a financial institution recorded in Part III but the financial institution's TIN was unknown, record the relationship but leave field 24a blank. If the subject has relationships with multiple Part III and Part IV financial institutions, complete a separate set of Item 24 fields for each financial institution. If more than one of 24h "Director," 24i "Employee," 24k "Officer," or 24l "Owner or Controlling Shareholder" is selected and/or the status or action date is different for each, an Item 24 for each must be completed.

25. If item 24h, i, k, or l is checked, indicate status of relationship

a. Relationship continues
b. Terminated
c. Suspended/barred
d. Resigned

Item 25. If item 24h, i, k, or l is selected: If any of boxes 24h, 24i, 24k, or 24l are selected, select the appropriate Item 25 option to indicate the status of the relationship. Select option 25a if the relationship continues. Select option 25b if the subject was terminated, 25c if the subject was suspended or barred, or 25d if the subject resigned. If multiple sets of Item 24 fields are completed on a subject, complete an Item 25 field for each set.

26. Action date MM/DD/YYYY if 25 b, c, or d is checked

Item 26 Action date: If any of boxes 25b through 25d have been checked, enter the date the action was taken. The date must be in MM/DD/YYYY format in a discrete FinCEN SAR and in YYYYMMDD format in a batch-filed FinCEN SAR. Leave Item 26 blank if no action was taken. If multiple Item 24 fields were created where box 25b, 25c, or 25d was checked, complete an Item 25 for each Item 24.

***** 27. Financial Institution TIN and account number(s) affected that are related to subject, if any.

a. (check if) No known account involved
b. (check if) Non-U.S. financial institution
c. TIN
d. account number
e. (check if) closed

Item 27 Financial institution TIN and acct. number(s) affected that are related to the subject, if any: Enter in Item 27 information about any accounts involved in the suspicious activity that are related to the subject recorded in Part I. Enter account numbers without formatting or special characters such as spaces, hyphens, or periods. See General Instruction 9 for information about entering account numbers in fields. An account is related to a subject if the subject owns the account, has control over the account, or conducted activity in or through an account the subject does not own or control. Check box 27a "No known acct. involved" if no account related to the subject is involved in the suspicious activity. Check box 27b "Non-US Financial Institution" if the account is located at a foreign financial institution. Enter in field 27c the TIN, if known, of the financial institution where the account is held. If the TIN is unknown leave the TIN field blank. Enter the account number involved in field 27d. If the account is closed, check the "Yes" box. If multiple account numbers are involved in the suspicious activity, complete an additional set of account number fields for each account number. Record account numbers involved in the suspicious activity that are related to the subject even if the TIN or name of the financial institution is unknown. If the TIN of a financial institution associated with an account number entered in 27d is unknown, record the institution name and

© gettechnical inc 2021

associated account number in Part V (example: “The account number 123654987 is held at First Federal Bank.”). If the filer is aware that the subject has an account involved in the suspicious activity with a financial institution listed in Part III but the account number is unknown, record the financial institution TIN in Item 27a but leave the associated account number field blank. Explain the missing account number in Part V. The subject’s relationship to any account recorded in Item 27 must be clearly defined in Part V unless the subject is the owner of the account (example: “The subject made unauthorized purchases using a stolen debit card for account 3456789 owned by his aunt.”).

28. . Subject’s role in suspicious activity (if applicable)

a. Purchaser/Sender
b. Payee/Receiver
c. Both a & b

Item 28 Subject's role: Record the subject's role in the suspicious activity by selecting the appropriate option. Select option 28a "Purchaser/Sender" if the subject purchased or sent the financial instrument(s) or product(s) involved in the suspicious activity. Select option 28b "Payee/Receiver" if the subject was the payee or receiver of the instrument(s) or product(s). Select option 28c "Both a & b" if the subject was both a purchaser/sender and payee/receiver. Instruments and products are not limited to the instruments and products listed in Items 45 and 46.

Note: Item 28 generally applies to institutions such as MSB’s or depository institutions through which the subject conducted transactions involving wire transfers, traveler’s checks, money orders, or like products/financial instruments

---------- Part II Suspicious Activity Information ----------

* 29. Amount involved in this report

a. (check if) Amount unknown
b. (check if) No amount involved

Item *29 Amount involved in this report: Enter the total dollar amount involved in the suspicious activity for the time period of this report. If the amount is unknown, leave this item blank and check box 29a "Amount unknown." Explain why the dollar amount is unknown in Part V. If some dollar amounts are known while others are unknown, enter the total of all known amounts and explain the unknown amounts in Part V. If there is no amount involved in the suspicious activity, check box 29b “No amount involved.” If the FinCEN SAR is a continuing report with box 1c "Continuing activity report" checked, enter only the amount involved for the time period covered by this FinCEN SAR. Do not include amounts from prior FinCEN SARs in Item 29. See General Instruction 9 for information on entering amounts.

*30. Date or date range of suspicious activity for this report

a. From: MM/DD/YYYY
b. To: MM/DD/YYYY

Item *30 Date or date range of suspicious activity for this report: Enter the suspicious activity date or date range for this report. If the suspicious activity occurred on a single day, enter that date in field 30a "From" and leave field 30b "To" blank. If the suspicious activity occurred on multiple days, enter the earliest date of suspicious activity in field 30a and the most-recent date of suspicious activity in field 30b. If the exact date(s) of the suspicious activity is (are) unknown, enter a date range that the filer believes will encompass the date(s) of the suspicious activity. Explain the nature of this date range in Part V. If the FinCEN SAR involves continuing activity with box 1c "Continuing activity report" checked, enter only the date range covered by this FinCEN SAR. Record in Part V the aggregated date range of all FinCEN SARs filed on the continuing suspicious activity. Use the format MM/DD/YYYY for dates in a discrete FinCEN SAR and the format YYYYMMDD for dates in a batch-filed FinCEN SAR.

31. Cumulative amount only if box 1c (continuing activity report) is checked

© gettechnical inc 2021

Item 31 Cumulative amount: Enter the cumulative amount involved in the suspicious activity in Item 31 if box 1c "Continuing activity report" is checked. The cumulative amount represents the total amount involved in all FinCEN SARs filed on the suspicious activity, including the current FinCEN SAR. If box 1c is checked and the cumulative dollar amount is unknown because all dollar amounts are unknown or no dollar amount is involved, enter zero (0) and explain the entry in Part V. If some dollar amounts are known while others are unknown, enter the total of all known amounts in Item 31 and explain the nature of the unknown amounts in Part V. See General Instruction 10 for information on entering amounts. Leave Item 31 blank if box 1c is not checked.

Items 32 - 41 Types of suspicious activity: Use the suspicious activity category Items 32 through **41** to record the type(s) of suspicious activity being reported. Check all boxes that apply to the suspicious activity. If a category applies but none of the options apply, check the category's box "z Other" and briefly describe the type of suspicious activity in the associated text field. If necessary, explain the type of suspicious activity in more detail in Part V.

Note: Items 32-41 are considered critical. At least one item in 32 to 41 must be checked.

32. Structuring
    a. Alters or cancels transaction to avoid BSA recordkeeping requirement
    b. Alters or cancels transaction to avoid CTR requirement
    c. Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements
    d. Transaction(s) below BSA recordkeeping threshold
    e. Transaction(s) below CTR threshold
    z. Other (specify type of suspicious activity in space provided)
33. Terrorist financing
    a. Known or suspected terrorist / terrorist organization
    z. Other (specify type of suspicious activity in space provided)
34. Fraud
    a. ACH
    b. Advance fee
    c. Business loan
    d. Check
    e. Consumer loan
    f. Credit/Debit card
    g. Healthcare/Public or private health insurance
    h. Mail
    i. Mass-marketing
    j. Ponzi scheme
    k. Pyramid scheme
    l. Securities fraud
    m. Wire
    z. Other (specify type of suspicious activity in space provided)
35. Gaming activities
    a. Chip walking
    b. Minimal gaming with large transactions
    c. Suspicious use of counter checks or markers
    d. Unknown source of chips
    z. Other (specify type of suspicious activity in space provided)

© gettechnical inc 2021

36. Money laundering

a. Exchanges small bills for large bills or vice versa
b. Funnel account
c. Suspicion concerning the physical condition of funds
d. Suspicion concerning the source of funds
e. Suspicious designation of beneficiaries, assignees or joint owners
f. Suspicious EFT/wire transfers
g. Suspicious exchange of currencies
h. Suspicious receipt of government payments/benefits
i. Suspicious use of multiple accounts
j. Suspicious use of noncash monetary instruments
k. Suspicious use of third-party transactors (straw-man)
l. Trade Based Money Laundering / Black Market Peso Exchange
m. Transaction out of pattern for customer(s)
z. Other (specify type of suspicious activity in space provided)

37. Identification / Documentation

a. Changes spelling or arrangement of name
b. Multiple individuals with same or similar identities
c. Provided questionable or false documentation
d. Provided questionable or false identification.
e. Refused or avoided request for documentation
f. Single individual with multiple identities
z. Other (specify type of suspicious activity in space provided)

38. Other suspicious activities

a. Account takeover
b. Bribery or gratuity
c. Counterfeit instruments
d. Elder financial exploitation
e. Embezzlement/theft/disappearance of funds
f. Forgeries
g. Human smuggling
h. Human trafficking
i. Identity theft
j. Little or no concern for product performance penalties, fees, or tax consequences
k. Misuse of position or self-dealing
l. Suspected public/private corruption (domestic)
m. Suspected public/private corruption (foreign)
n. Suspicious use of informal value transfer system
o. Suspicious use of multiple transaction locations
p. Transaction with no apparent economic, business, or lawful purpose
q. Transaction(s) involving foreign high risk jurisdiction
r. Two or more individuals working together
s. Unlicensed or unregistered MSB
z. Other (specify type of suspicious activity in space provided)

© gettechnical inc 2021

39. Insurance

a. Excessive insurance
b. Excessive or unusual cash borrowing against policy/annuity
c. Proceeds sent to or received from unrelated third party
d. Suspicious life settlement sales insurance (e.g. STOLIs, Viaticals)
e. Suspicious termination of policy or contract
f. Unclear or no insurable interest
z. Other (specify type of suspicious activity in space provided

40. Securities / Futures / Options

a. Insider trading
b. Market manipulation
c. Misappropriation
d. Unauthorized pooling
e. Wash Trading
z. Other (specify type of suspicious activity in space provided)

41. Mortgage fraud

a. Application fraud
b. Appraisal fraud
c. Foreclosure/Short sale fraud
d. Loan modification fraud
e. Origination fraud
z. Other (specify type of suspicious activity in space provided)

42. Cyber event (If reporting)

a. Against Financial Institution(s)
b. Against Financial Institution Customer(s)
z. Other (specify type of suspicious activity in space provided)

Item 42, Cyber event: Complete item 42 to indicate if the cyber event was directed against the financial institution or its customer/account holder. Events against the institution may include, but not limited to, a digital denial of service (DDoS), an attempt to break (hack) into the financial institutions computer system or an attempt to take over the financial institutions "wire transfer system," the financial institutions website, a Business E-Mail Attack (BEA), etc.

Examples of cyber events against the financial institutions customer may include the takeover (or attempted takeover) of the customer's account, the sending of bogus e-mails that appear to come from the customer directing various financial transactions that do not follow the customers normal account activity, etc.

43. IP Address(es) (if available, multiples up to 99)

a. Date (MM/DD/YYYY)
b. Time Stamp (UTC) HH:MM:SS

Item 43 IP address: If known, enter the IP address of the subject's electronic internet based contact with the financial institution. For example, this may be the IP address used to log into the institution's online

© gettechnical inc 2021

banking page or the IP address used to access an institution's mobile application. In item 43a enter the date (MM/DD/YYYY format) of the activity. In 43b enter the UTC time in (HH:MM:SS format) of the first instance of the reported IP address. Select the (+) sign to report multiple IP address, date and time information. IP address information must be explained in the FinCEN SAR Part V narrative. Batch filers will use the date format YYYYMMDD.

NOTE: If reporting an IP address in connection with a cyber-event, complete item 44.

Item 44. Cyber-event indicator (multiple entries up to 99)

Item 44 Cyber-event indicator: Enter the cyber-event indicator by selecting the appropriate indicator from the dropdown list provided and enter the supporting information in the associated text field (an indicator not listed may be entered in the "z" Other text fields. Select the (+) sign to report multiple event indicators. Each cyber-event indicator and its associated text field is limited to 99 entries. Cyber-event indicator information must be explained in the BFinCEN SAR Part V narrative. See General Instruction 13 for additional information on reporting cyber-related events.

44a. Command and Control IP address

44a1 Event value text field (each entry of 44a must have a corresponding event value text field).

44a2 Event value text field (Date associated with the value in 44a1).

44a3 Event value text field (Timestamp associated with the value in 44a1).

44b. Command & Control URL/Domain

44b1 Event value text field. (each entry of 44b must have a corresponding event value text field)

44c. Malware MD5, Malware SHA-1, or Malware SHA-256.

44c1 Event value text field. (each entry of 44c must have a corresponding event value text field)

44d. Media Access Control (MAC) Address

44d1 Event value text field (each entry of 44d must have a corresponding event value text field).

44e. Port

44e1 Event value text field. (each entry of 44e must have a corresponding event value text field)

44f. Suspicious e-mail address

44f1 Event value text field. (each entry of 44f must have a corresponding event value text field)

44g. Suspicious filename

44g1 Event value text field. (each entry of 44g must have a corresponding event value text field)

44h. Suspicious IP Address

44h1 Event value text field. (each entry of 44h must have a corresponding event value text field)

44h2 Event value Date associated with the value in 44h1 (discrete format MM/DD/YYYY and batch format YYYYMMDD).

44h3 Event value Timestamp associated with the value in 44h1.

44i. Suspicious URL/Domain

44i1 Event value text field. (each entry of 44i must have a corresponding event value text field)

© gettechnical inc 2021

44j. Targeted system

44j1 Event value text field. (each entry of 44j must have a corresponding event value text field)

44z. Other

44z Text description of Other value

44z1 Event value text field. (each entry of 44z must have a corresponding event value text field)

45. Were any of the following product type(s) involved in the suspicious activity? Check all that apply:

a. Bonds/Notes
b. Commercial mortgage
c. Commercial paper
d. Credit card
e. Debit card
f. Deposit account
g. Forex transactions
h. Futures/Options on futures
i. Hedge fund
j. Home equity line of credit
k. Home equity loan
l. Insurance/Annuity products
m. Microcap securities
n. Mutual fund
o. Options on securities
p. Prepaid access
q. Residential mortgage
r. Security futures products
s. Stocks
t. Swap, hybrid or other derivative
z. Other (specify type in space provided)

Item 45 Product types involved in suspicious activity: Check all Item 45 boxes that apply to record the product type(s) involved in the suspicious activity. Option 45f 'Forex transactions" includes all foreign exchange transactions both on and off-exchange, including futures and options on foreign exchange. Option 45g "Futures/Options on futures" includes futures and options on any "commodity," as that term is defined in Section 1a(4) of the Commodity Exchange Act, including broad-based security indexes. Option 45s "Swap, hybrid or other derivative" includes all derivatives not included above including those traded over-the-counter and off-exchange. If the product type is not covered by options 45a through 45s, check box 45z "Other (list below)" and enter a brief description in the associated text field. If necessary provide a more detailed product type (such as commodity futures contracts, options on commodity futures contracts, commodity options, and OTC agricultural trade options) in Item 48 "Product/instrument description" or in Part V. If there are multiple product types not covered by Item 45, record one in Item 45z "Other (List below)" and all others in Part V.

46. Were any of the following instrument type(s)/payment mechanism(s) involved in the suspicious activity? Check all that apply:

a. Bank/cashier's check
b. Foreign currency
c. Funds transfer
d. Gaming instruments
e. Government payment

© gettechnical inc 2021

f. Money orders
g. Personal/Business check
h. Travelers checks
i. U.S. Currency
z. Other (specify type in space provided)

Item 46 Instrument types involved in suspicious activity: Check all Item 46 boxes that apply to record the instrument type(s) involved in the suspicious activity. If the instrument type is not covered by options 46a through 46i, check box 46z "Other (List below)" and enter a brief description in the associated text field. If necessary provide a more- detailed description of the instrument type in Part V. If there are multiple instrument types not covered by Item 46, record one in Item 46 "Other (List below)" and all others in Part V.

47. Commodity type (if applicable)

Item 47 Commodity type: If a commodity is involved in the suspicious activity, record the commodity type in Item Multiple Item 47 fields should be completed if multiple commodity types are involved in the suspicious activity.

48 Product/Instrument description (if needed) (multiple entries up to 99)

Item 48 Product description: Provide a description of the product recorded in Item 45 or instrument recorded in Item 46 if necessary for a more-complete understanding of the suspicious activity. Multiple Item 48 fields should be completed if multiple products or instruments requiring a description are involved in the suspicious activity.

49. Market where traded

Item 49 Market where traded: Enter in Item 49 the three to five-letter code for the market where a commodity recorded in Items 45 or 47 was traded. Multiple Item 49 fields should be completed if multiple markets are involved in the suspicious activity. Use only the ISO 10383 Exchange/Market Identifier Codes (MIC) found at http://www.iso15022.org/MIC/homepageMIC.htm.

50. CUSIP number

Item 50 CUSIP® number: Enter in Item 50 the CUSIP® (Committee on Uniform Securities Identification Procedures) number of any securities products such as stocks and bonds involved in the suspicious activity. Multiple Item 50 fields should be completed if there are multiple CUSIP numbers for multiple securities products involved in the suspicious activity.

---------- Part III Information about Financial Institution Where Activity Occurred ----------

Part III records information about the financial institution(s) where the suspicious activity occurred. Complete a separate Part III record on each financial institution involved in the suspicious activity. If box 1d "Joint report" is checked there must be two or more Part III records in the FinCEN SAR, one for the Part IV filing institution or filer subsidiary and one for each joint filer. If a financial institution recorded in Part III has branches involved in the suspicious activity, record the branch information in Items 68 through 74. Information for up to 99 branches can be recorded in a single FinCEN SAR. A branch is a location (such as an office or ATM) owned by the financial institution but located separately from the financial institution's headquarters. If a reporting financial institution has agents where the suspicious activity occurred, a separate Part III must be prepared on each agent. An agent is an independent financial institution (such as a supermarket that sells money orders or an independent insurance agent) that has a contractual relationship with the reporting financial institution to conduct financial transactions. Do not place agent information in branch fields. Generally, branch operates under the same TIN as the financial institution. An agent has a TIN different from the financial institution. Financial institution as used in Part III includes individuals acting as sole proprietorship financial institutions using their personal Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN).

*51. Type of financial institution

© gettechnical inc 2021

a. Casino/Card club
b. Depository institution
c. Insurance company
d. MSB
e. Securities/Futures
f. Loan or Finance Company
g. Housing GSE
z. Other (specify type of institution in space provided)

Item *51 - Type of financial institution: Select the appropriate type of financial institution that best describes the financial institution recorded in Item 51. If none of those options apply, select "Other" and enter a brief description in the associated text field. If necessary, include a more- detailed description in Part V.

NOTE: If the financial institution is a dealer in precious metals, stones, or jewels, select option "Other" and enter "DEALER IN PRECIOUS METALS STONES JEWELS" in the associated text field.

*52. Primary Federal Regulator

a. CFTC
b. Federal Reserve
c. FDIC
d. IRS
e. NCUA
f. OCC
g. SEC
z. Not Applicable

Item *52 Primary federal regulator: Select the appropriate option to identify the primary federal regulator or BSA examiner of the financial institution recorded in Part III. If more than one regulator option could apply, enter the code for the regulator that has primary responsibility for enforcing compliance with the BSA. If Item 51 option "Casino/Card Club," "Insurance Company," or "MSB" was selected, the Item 52 entry must be "Internal Revenue Service (IRS)." If the institution recorded in Part III is subject to U.S. law and none of the other codes apply, select option "Internal Revenue Service (IRS)." If the institution recorded in Part III is not subject to U.S. law, then select option "Not Applicable."

53. If item 51a is checked, indicate type of gaming institution (check only one)

a. State licensed casino
b. Tribal authorized casino
c. Card club
z. Other (specify type of gaming institution in space provided)

Item 53 Gaming institution type: If option 51a was selected indicating the financial institution is a gaming institution such as a casino or card club, record the type of gaming institution by checking the appropriate box. If

© gettechnical inc 2021

none of the options 53a through 53c are appropriate, check box 53z "Other" and provide a brief description in the associated text field. If necessary, include a more detailed description in Part V.

54. If item 51e is checked, indicate type of Securities and Futures institution or individual where activity occurred - check the boxes of all types that apply to this report.

a. Clearing broker – securities
b. Execution-only broker securities
c. Futures commission merchant
d. Holding company
e. Introducing broker - commodities
f. Introducing broker - securities
g. Investment adviser
h. Investment company
i. Retail foreign exchange dealer
j. Self-clearing broker-securities
k. Subsidiary of financial/bank holding company
z. Other (specify type of institution or individual in space provided)

Item 54 Securities and futures type: If option 51e was checked indicating the financial institution is part of the securities and futures industries, check all boxes that apply to the reported suspicious activity. If none of options 54a through 54k apply, check box 54z "Other" and record a brief description of the type in the associated text field. Examples of this are commodity pool operator or commodity trading adviser. If necessary, include a more-detailed description in Part V.

55. Financial institution identification number

a. Central Registration Depository (CRD) number
b. Investment Adviser Registration Depository (IARD) number
c. National Futures Association (NFA) number
d. Research, Statistics, Supervision, and Discount (RSSD) number
e. Securities and Exchange Commission (SEC) number
f. National Association of Insurance Commissioners (NAIC Code)
g. Mortgage (NMLS ID)
z. Identification number

Item 55 Financial institution identification number: Select the appropriate option if the financial institution recorded in Part III has a Central Registration Depository (CRD) number, an Investment Adviser Registration Depository (IARD) number, a National Futures Association (NFA) number, a Research Statistics Supervision Discount (RSSD) number, National Association of Insurance Commissioners (NAIC Code), Mortgage (NMLS ID) or a Securities and Exchange Commission (SEC) Reporting File Number (RFN). Do not enter an SEC Central Index Key (CIK) number in place of the RFN. Record the number in field 55h. See General Instruction 8 for information on entering identifying numbers.

56. Financial institution's role in transaction (if applicable)

a. (check if) Selling location
b. (check if) Paying location
c. (check if) Both a & b

Item 56 Financial institution role in transaction: Check the box "Selling location" if the customer purchased at the Part III financial institution the products or instruments recorded in Items 45 **or 46**. Check the box "Paying location" if the customer received payment from the Part III financial institution for the products or instruments recorded in

© gettechnical inc 2021

Items 45 or 46. Check the box “Both” if the Part III financial institution was both a paying and selling location for the products or instruments recorded in Items 45 or 46.

Note: Item 56 generally applies to institutions such as MSB’s or depository institutions through which the subject conducted transactions involving wire transfers, traveler’s checks, money orders, or like products/financial instruments.”

*57. Legal name of financial institution

a. (check if) unknown

Item 57 Legal name of financial institution: Enter the legal name of the financial institution as recorded on articles of incorporation or other documents establishing the institution. Record as the legal name the full name of an individual, such as a sole proprietorship, acting as a financial institution. Enter the individual’s name in (first name) (middle name) (last name) or equivalent format, e.g. John Jacob Doe or Richard R. Roe II, etc. Check box 57a “Unknown” if the legal name is unknown and leave Item 57 blank.

58. Alternate name, e.g., AKA if individual; DBA/trade name if entity

Item 58 Alternate name: If the financial institution recorded in Item 58 has a separate doing business as (DBA) name, enter that name here. If an individual recorded in Item 58 has a separate also known as (AKA) name, enter that name here also. Do not include the acronyms DBA or AKA with the alternate name.

* 59. TIN
a. (check if) unknown

Item 59 - TIN: Enter the Taxpayer Identification Number (TIN), either U.S. or foreign, of the financial institution or individual recorded in Item 57. See General Instruction 8 for information on entering identifying numbers. Check box 59a “Unknown” if the TIN is unknown and leave Item 59 blank.

60 TIN type
a. EIN
b. SSN-ITIN
c. Foreign

Item 60 TIN type: Select the option for the type of TIN entered in Item 59. If the TIN in Item 59 is unknown and the Item 57 financial institution has a U.S. address, select TIN Type option “EIN” if the financial institution is an entity and “SSN-ITIN” if the financial institution is an individual. If the financial institution has a foreign address and the TIN is unknown, select “Foreign.”

Items *61 - *65 Financial institution address items: Enter the financial institution's permanent street address, city, two or three letter state/territory/province code (U.S./Canada/Mexico only), ZIP Code or foreign postal code, and two letter country code. If an address item is unknown, leave that item blank and check the item’s "Unknown" box. Leave Item 63 State blank if the state is unknown or the country is not the U.S. or a U.S. Territory, Canada, or Mexico. See General Instruction 6 and the Part III introductory instructions for additional information on entering address data.

*61. Address

© gettechnical inc 2021

a. (check if) unknown

*62. City

a. (check if) unknown

63 State

*64. ZIP/Postal Code

a. (check if) unknown

*65. Country

66. Internal control/file number

Item 66 Internal control/file number: Enter the internal control number or file number, if applicable, assigned to the FinCEN SAR by the financial institution. This number should be unique to the FinCEN SAR if possible, allowing interested parties such as law enforcement or the financial institution to reference the FinCEN SAR without committing a potentially illegal disclosure of FinCEN SAR data.

67 Loss to financial institution (if applicable)

Item 67 Loss to financial institution: If the financial institution has suffered a loss because of the suspicious activity, record the amount of loss in Item 67. If some losses are known and other losses unknown, enter the total of known losses as of the date of filing. If the FinCEN SAR is a continuing FinCEN SAR because box 1c was checked, enter the loss amount for the current FinCEN SAR in Item 67 and record in Part V the total aggregated losses for all FinCEN SARs filed on the suspicious activity. The amount entered in this field cannot be zero and cannot be greater than the amount in Item 29 "Amount involved in this report." See General Instruction 10 for information on entering amounts.

68 Branch's role in transaction (if applicable)

a. (check if) Selling location
b. (check if) Paying location
c. (check if) Both a & b

Item 68 Branch's role: Check the box "Selling location" if the branch sold the products or instruments recorded in Items 45 or 46 to a customer. Check the box "Paying location" if a customer received payment from the branch for the products or instruments recorded in Items 45 or 46. Check the box "Both" if the Part III financial institution branch was both a paying and selling location for the products or instruments recorded in Items 45 or 46. This item must be blank if no branch is involved in the suspicious activity. If multiple branches are involved in the suspicious activity, a separate Item 68 must be prepared for each branch.

Note: Item 68 generally applies to institutions such as MSB's or depository institutions through which the subject conducted transactions involving wire transfers, traveler's checks, money orders, or like products/financial instruments.

© gettechnical inc 2021

Items *69 and 71-74 Branch address items: See the instructions for Items *61 - *65, the Part III introductory instructions, and General Instruction 6 for information on entering branch address data. If a branch address item is unknown, leave that item blank. Item 74 "Country" cannot be blank if any other branch address information is recorded. If no branch was involved in the suspicious activity or the branch country is unknown, check box 69a and leave the branch address items blank. If multiple branches are involved in the suspicious activity, complete a set of branch address items for each branch.

69 Address of branch or office where activity occurred

d. If no branch activity involved, check this box

70 RSSD number (of the Branch)

Item 70 RSSD number: Enter the RSSD (Research Statistics Supervision Discount) number of the branch, if known. If multiple branches are involved in the suspicious activity, complete Item 70 for each branch for which the RSSD number is known.

71 City

72 State

73 ZIP/Postal Code

*74. Country

---------- Part IV Filing Institution Contact Information ----------

Part IV records information about the lead financial institution, holding company, agency, or other entity that is filing the FinCEN SAR. There must be only one Part IV record in a FinCEN SAR. Do not include information about joint filers in a Part IV record. Joint filer information must be reported in a Part III record. Financial institution as used in Part IV includes individuals acting as sole proprietorship financial institutions using their personal Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN).

*75. Primary Federal Regulator (instructions specify banking agencies, SEC, CFTC, IRS)

a. Commodities Futures Trading Commission (CFTC)
b. Federal Reserve Board (FRB)
c. Federal Deposit Insurance Corporation (FDIC)
d. Internal Revenue Service (IRS)
e. National Credit Union Administration (NCUA)
f. Office of the Comptroller of the Currency (OCC)
g. Securities and Exchange Commission (SEC)
h. Federal Housing Finance Agency (FHFA)
z. Not Applicable.

Item *75 Primary federal regulator: Select the appropriate option from the drop-down list to identify the Primary Federal Regulator or BSA Examiner of the filing institution. If more than one regulator option could apply, select the regulator that has primary responsibility for enforcing compliance with the BSA. If Item 79 option "Casino/Card Club," "Insurance Company," or "MSB" is selected, the Item 75 entry must be "Internal Revenue Service (IRS)." If the financial institution filing the FinCEN SAR is subject to U.S. law and none of the other codes apply, the entry must

© gettechnical inc 2021

be “Internal Revenue Service (IRS).” If the FinCEN SAR is being filed by a government agency or if the financial institution filing the FinCEN SAR is not subject to U.S. law, the entry must be "Not Applicable.”

*76. Filer name (Holding company, lead financial institution, or agency, if applicable).

Item *76 Filer name: Enter the legal name of the filing institution as recorded on articles of incorporation or other documents establishing the institution. Enter the full name of the filer if the filer is an individual, such as a sole proprietorship, acting as a financial institution. If an individual’s name is recorded, enter the name in (first name) (middle name) (last name) or equivalent format, e.g. John Jacob Doe or Richard R. Roe II, etc.

*77. TIN

Item *77 - TIN: Enter the Taxpayer Identification Number (TIN), either U.S. or foreign, of the financial institution or individual recorded in Item 76. See General Instruction 8 for information on entering identifying numbers.

*78. TIN type

a. EIN
b. SSN/ITIN
c. Foreign

Item *78 - TIN type: Record the type of TIN entered in Item 77 by selecting the appropriate option.

*79. Type of financial institution

a. Casino/Card club
b. Depository institution
c. Insurance company
d. MSB
e. Securities/Futures
f. Loan or Finance Company
g. Housing GSE
z. Other (specify type of institution in space provided)

Item *79 - Type of financial institution: Select the appropriate type of financial institution that best describes the filing institution recorded in Item 76. If none of those options apply, select “Other” and enter a brief description in the associated text field. If necessary, include a more- detailed description in Part V.

NOTE: If the financial institution is a dealer in precious metals, stones, or jewels, select option “Other” and enter “DEALER IN PRECIOUS METALS STONES JEWELS” in the associated text field.

80 Type of Securities and Futures institution or individual filing this report - check the boxes of all types that apply to this report.

a. Clearing broker - securities
b. CPO/CTA
c. Execution-only broker securities
d. Futures commission merchant
e. Holding company
f. Introducing broker - commodities
g. Introducing broker - securities
h. Investment adviser

© gettechnical inc 2021

i. Investment company
j. Retail foreign exchange dealer
k. Self-clearing broker-securities
l. SRO Futures
m. SRO Securities
n. Subsidiary of financial/bank holding company
z. Other (specify type of institution or individual in space provided)

Item 80 - Securities and futures type: If option 80e “Securities/Futures” was selected, check all boxes that apply to indicate the type of securities and futures institution that is filing the FinCEN SAR. If none of options 80a through 80nl apply, check box 80z "Other" and record a brief description of the type in the associated text field. If necessary, include a more-detailed description in Part V.

81. Filing institution identification number

a. Central Registration Depository (CRD) number
b. Investment Adviser Registration Depository (IARD) number
c. National Futures Association (NFA) number
d. Research, Statistics, Supervision, and Discount (RSSD) number
e. Securities and Exchange Commission (SEC) number
f. National Association of Insurance Commissioners (NAIC Code)
g. Mortgage (NMLS ID)

z. Identification number

Item 81 - Filing institution identification number: See instructions for Item 55. Items 82-86 - Address: See instructions for Items 61 through 65.

*82. Address

* 83. City

*84. State

* 85. ZIP/Postal Code

* 86. Country

87 Alternate name, e.g., AKA if individual; DBA/ trade name if entity. See instructions for Item 58.

88 Internal control/file number: See instructions for Item 66.

89 LE contact agency

Item 89 - LE contact agency: Enter the name of the law enforcement agency, if any, which has been informed of the suspicious activity.

NOTE: If more than one LE agency has been contacted about the suspicious activity, record the information on one agency in Items 89-92 and the information on additional agencies in Part V.

90 LE contact name

Item 90 - LE contact name: Enter the name of the person contacted at the law enforcement agency.

91 LE contact phone number

© gettechnical inc 2021

Item 91 - LE contact phone number: Enter the law enforcement contact telephone number. See General Instruction 7 for information on entering telephone numbers.

91a. Extension (if any)

Item 91a - Extension: Enter the extension, if any, of the law enforcement contact telephone number

92 LE contact date

Item 92 – LE contact date: Enter the most-recent date the law enforcement agency was contacted about the suspicious activity. If the agency was contacted on multiple dates, record the earlier contact dates in Part V. Discrete filers will use the format MM/DD/YYYY while batch filers will use the format YYYYMMDD.

*93. Filing institution contact office

Item 93 - Filing institution contact office: Enter the name of the filing institution contact office where additional information about the FinCEN SAR or supporting documentation can be requested. If the FinCEN SAR is jointly filed, enter in Part V the contact office and telephone number information for all Part III joint filers.

*94. Filing institution contact office phone number including area code

a. Extension, if any

Item 94 - Filing institution contact office phone number: Enter the contact office telephone number. See General Instruction 7 for additional instructions on entering telephone numbers.

Item 94a - Extension: Enter the extension, if any, of the contact office telephone number.

*95. Date filed

Item 95 - Date filed: Enter the date the FinCEN SAR is filed. This date will be entered automatically when a discrete FinCEN SAR is electronically filed. Batch filers will report this date in YYYYMMDD format.

---------- * Part V Suspicious Activity Information – Narrative ----------

The narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion. This description should encompass the data provided in Parts I through III, but should include any other information necessary to explain the nature and circumstances of the suspicious activity. Filers should provide any information the filers believe necessary to better enable investigators to understand the reported suspicious activity. Narratives must be completed in English. Filers should use the following checklist as a guide for preparing the narrative:

- If filers have additional information pertaining to items in Parts I through IV this information should be recorded in the narrative and referenced to the item number.
- If this report is a corrected or amended report, complete the report in its entirety with whatever corrections or amendments were required. Describe the corrections or amendments at the beginning of the narrative.
- If this report is a continuing report, describe the circumstances surrounding the suspicious activity

© gettechnical inc 2021

for the 90-day period encompassing the report. Include information from prior FinCEN SAR narratives only when it is necessary for an understanding of the nature and circumstances of the suspicious activity. Never include the entire narratives of the prior FinCEN SARs.

- If any item in the report was insufficient for recording all item data held by the filer, or if an item's instructions require entry of additional data or explanation in the narrative, record the additional data referenced by item number in the narrative.
- Information provided in other sections of the FinCEN SAR need not be repeated in the narrative unless necessary to provide a clear and complete description of the suspicious activity.
- Describe the conduct or transaction(s) that caused suspicion. If appropriate, this description should be chronological when the activity involves multiple instances or encompasses more than one day.
- Explain whether any transaction(s) involved were completed or only attempted.
- Explain who benefited and how they benefited, financially or otherwise, from the activity.
- Describe all supporting documentation and retain the documentation for five years. DO NOT include supporting documentation with the FinCEN SAR. (See General Instruction 6.)
- If the FinCEN SAR is jointly-filed, name all joint filers and describe the nature of supporting document held by the joint filers. Provide the contact office name and telephone number for each joint filer.
- Describe and retain any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others
- Describe and retain any admission or explanation of the activity or transaction(s) provided by the subject(s), witness(s), or other person(s), including to whom and when it was given.
- Indicate where the suspicious activity took place, e.g. branch, cage, gaming pit, agent location, etc.
- Indicate whether the suspicious activity is an isolated incident or related to other activity.
- Indicate whether any U.S. or foreign currency or other negotiable instruments were involved. If foreign currency or other foreign instruments, provide the foreign amount, currency name, and country of origin.
- Indicate if there is any litigation related to the activity by specifying the name of the litigation and court where the action is pending.
- Describe the nature of losses and recoveries related to the suspicious activity, including aggregated losses and recoveries in continuing activity.
- Identify the names of financial institutions associated with account numbers when the financial institution TINs were unknown.
- If the subject is a foreign national provide all available information on the subject's passport(s), visa(s), and other identification. Include identifying data such as issuing date, country, document numbers, issuing authority, and nationality.
- If the suspicious activity involves transfers of funds to or from a foreign country or currency exchanges involving foreign currencies, identify the foreign currency, country of issue, and the source or destination of the funds.
- If a subject involved in the suspicious activity has an insider relationship with a financial institution, describe the subject's position with the financial institution and how that position related to the suspicious activity.
- Provide information on the victims of the suspicious activity only when it is necessary for a complete understanding of the activity. DO NOT record victim information in a Part I Subject Information record.
- Provide information about the financial institution's business policies and practices only if it is necessary for a complete understanding of the suspicious activity. DO NOT include legal disclaimers in the narrative.
- Do not include tabular data in a FinCEN SAR narrative. Such data should be reported in an appropriate comma separated values attachment.

© gettechnical inc 2021

Filers can include with a FinCEN SAR an attachment containing tabular data (such as transaction data) that provides additional suspicious activity information not suitable for inclusion in the narrative. This file must be an MS Excel-compatible comma separated value (CSV) file with a maximum size of 1 megabyte. Discrete FinCEN SAR filers can attach this file by clicking the "Add Attachment" button on the discrete FinCEN SAR header page and following the instructions provided. Batch filers must follow the instructions in Attachment D – Batch Attachments to add CSV files to a batch file.

© gettechnical inc 2021

10. Attachment D – Secure Data Transfer Mode Filers

FinCEN provides the ability for filers to submit the FinCEN SAR XML batch file securely via the Internet using a VPN device or Connect:Direct software. This method of filing is referred to as Secure Data Transfer Mode (SDTM). SDTM allows for a secure, system to system mechanism for transferring batch submissions from your organization's internal server to the BSA E-Filing server. The batch submission process can be automated such that user intervention/involvement is minimized. There is no interaction with the BSA E-Filing system web site for the upload of the batch file but the BSA E-Filing system web site is used to track the status of the submissions.

For filers using this option for filing, SDTM filers can submit a single file containing the FinCEN SAR XML batch data. The file naming convention is as follows:

Submission type: SARXST

Date/Time: This will be a date-time stamp to guarantee filename uniqueness

- Year = YYYY
- Month = MM
- Day = DD
- Hour = hh
- Minute = mm
- Second = ss

Organization name: Custom naming by the submitting organization (e.g. "ABCPreparingFirm")

Extension: xml

Example FinCEN SAR XML batch file name: SARXST.20170609153015.ABCPreparingFirm.xml

Corresponding FinCEN SAR XML batch Acknowledgement file name: This file name will match the corresponding input FinCEN SAR XML batch file name with the text "*.ACKED" appended to the end.

For example: SARXST.20170609153015.ABCPreparingFirm.xml.ACKED

For more information on how to setup an SDTM connection, please refer to the SDTM Requirements documentation available on the BSA E-Filing System secure side, or you may contact the BSA E-Filing Help Desk at 1-866-346-9478 or via email at BSAEFilingHelp@fincen.gov. The Help Desk is available Monday through Friday from 8 a.m. to 6 p.m. EST. Please note that the Help Desk is closed on Federal holidays.

© gettechnical inc 2021

11. Attachment E – Supporting Documentation (Attachments)

Institutions filing electronic FinCEN Suspicious Activity Reports (FinCEN SAR) may, but are not required to, attach a Microsoft Excel-compatible comma separated values (CSV) file (no larger than 1 MB) providing details in tabular form of transactions subject to the suspicious activity discussed in Part V "Narrative Description" of the FinCEN SAR.

NOTE: Please be advised that when entering data into an Excel spreadsheet prior to saving it as a comma separated (.CSV) file, the default behavior for numeric data entered into cells is to convert numeric values over 11 characters into scientific notation. For example, the value of 123456789123 is converted to 1.23457E+11 after entry. When the Excel spreadsheet is saved to a comma separated (.CSV) fill, this visible format is retained and when opened the entire original number is not displayed, 123456789123, but rather 1.23457E+11. To avoid this behavior, please ensure that your workbook cells are formatted as text prior to entering data in the cell. This can be accomplished by selecting the column, right clicking the mouse and selecting Format Cells, and then selecting Text under Category, and then OK. This must be done before entering the data, not after.

While the BSA E-Filing System limits the number of attachments for a single FinCEN SAR to one (1) CSV file, batch filers must abide by the following instructions in order to submit attachments for one or more FinCEN SAR within their batch file:

1. **Record the supporting document file name for each FinCEN SAR XML within the batch**

Record the <ActivitySupportDocument> element, along with the <OriginalAttachmentFileName> sub-element, for each FinCEN SAR Activity within the XML batch associated with an attachment. Record the full name of the corresponding CSV file within the OriginalAttachmentFileName element.

2. **Record the counts for the total number of attachments and FinCEN SAR XML activities with attachments with the batch**

   Record the following attributes and counts within the EFilingBatchXML element in the XML batch:

   - ActivityAttachmentCount. The count of all <Activity> elements in the batch where the <OriginalAttachmentFileName> element is recorded with a value referencing the file name of the FinCEN SAR attachment
   - AttachmentCount. The count of all <OriginalAttachmentFileName> elements in the batch that contain a value referencing the file name of the FinCEN SAR attachment

3. **Include all attachments in a single zip file with the FinCEN SAR XML activity sequence number appended to each attachment file name**

   - Create a zip file composed of all attachments. When naming the zip file, be sure to use a descriptive file name to help you identify which FinCEN SAR batch your attachment zip file is associated with.
   - For each csv attachment file within the zip file, append the corresponding sequence number (i.e. "SeqNum" value associated with the FinCEN SAR Activity in the XML batch as follows:

     <FinCEN SAR Activity SeqNum>_<OriginalAttachmentFileName>.csv

     For example:
     1_BankofUSBatchAttachment.csv

© gettechnical inc 2021

The above example indicates that within the FinCEN SAR XML batch, Activity SeqNum="1" contains the <OriginalAttachmentFileName> element with the value of "BankofUSBatchAttachment.csv".

4. **Attach the attachments zip file to the FinCEN SAR XML Batch Form prior to submission**

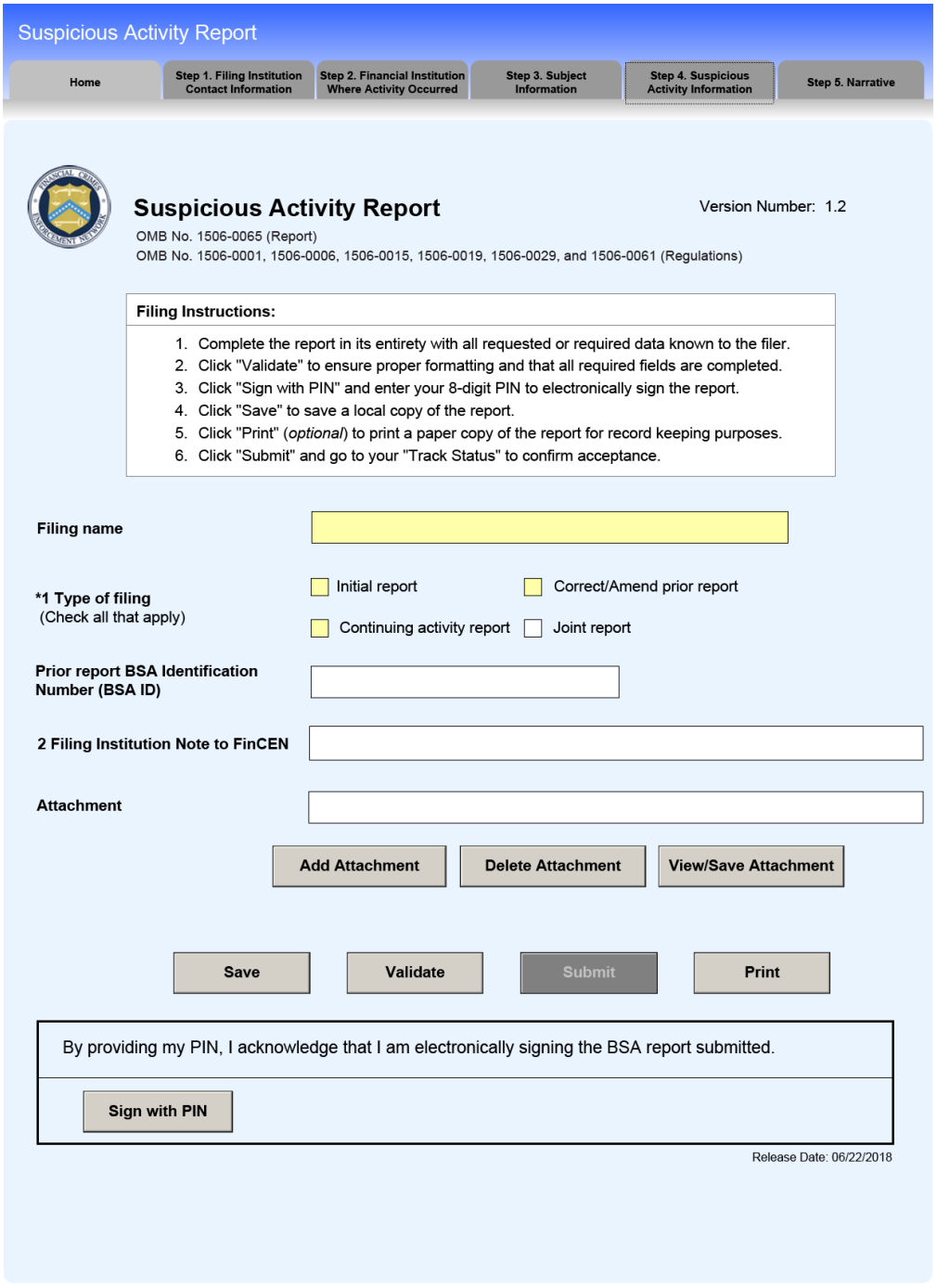
Once all required fields are complete and your FinCEN SAR XML batch has been attached to the FinCEN SAR XML Batch Form, locate the Add File button for attachments in order to add your attachment zip file to the FinCEN SAR XML Batch Form. Once the attachment file is attached, you may sign the FinCEN SAR Batch Form with your PIN, save, and submit.

ATTENTION: Secure Data Transfer Mode (SDTM) Filers

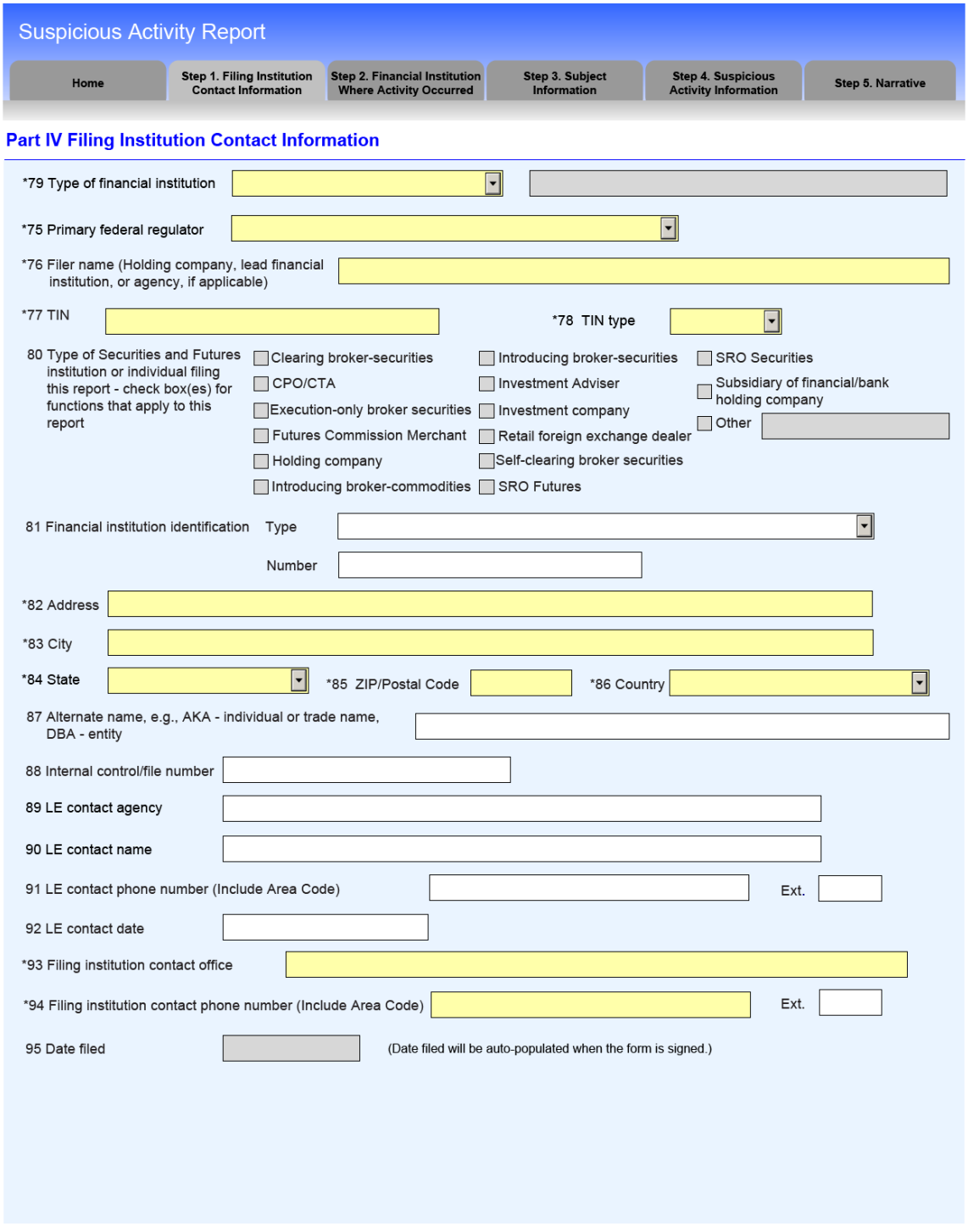
Filers who transmit the FinCEN SAR XML batch data via secure server-to-server connection may submit a single ZIP file containing the FinCEN SAR XML batch file along with the corresponding attachment zip file. This single ZIP file is composed of one FinCEN SAR XML batch file and one attachment ZIP file. The attachment ZIP file shall follow the same attachment requirements described above. The single ZIP file name must start with "SARXST." and end with ".ZIP". For example: SARXST.SARXML_batch.ZIP. FinCEN SAR XML SDTM batch files without any attachment shall follow the naming convention described in Attachment D of this guide.

© gettechnical inc 2021

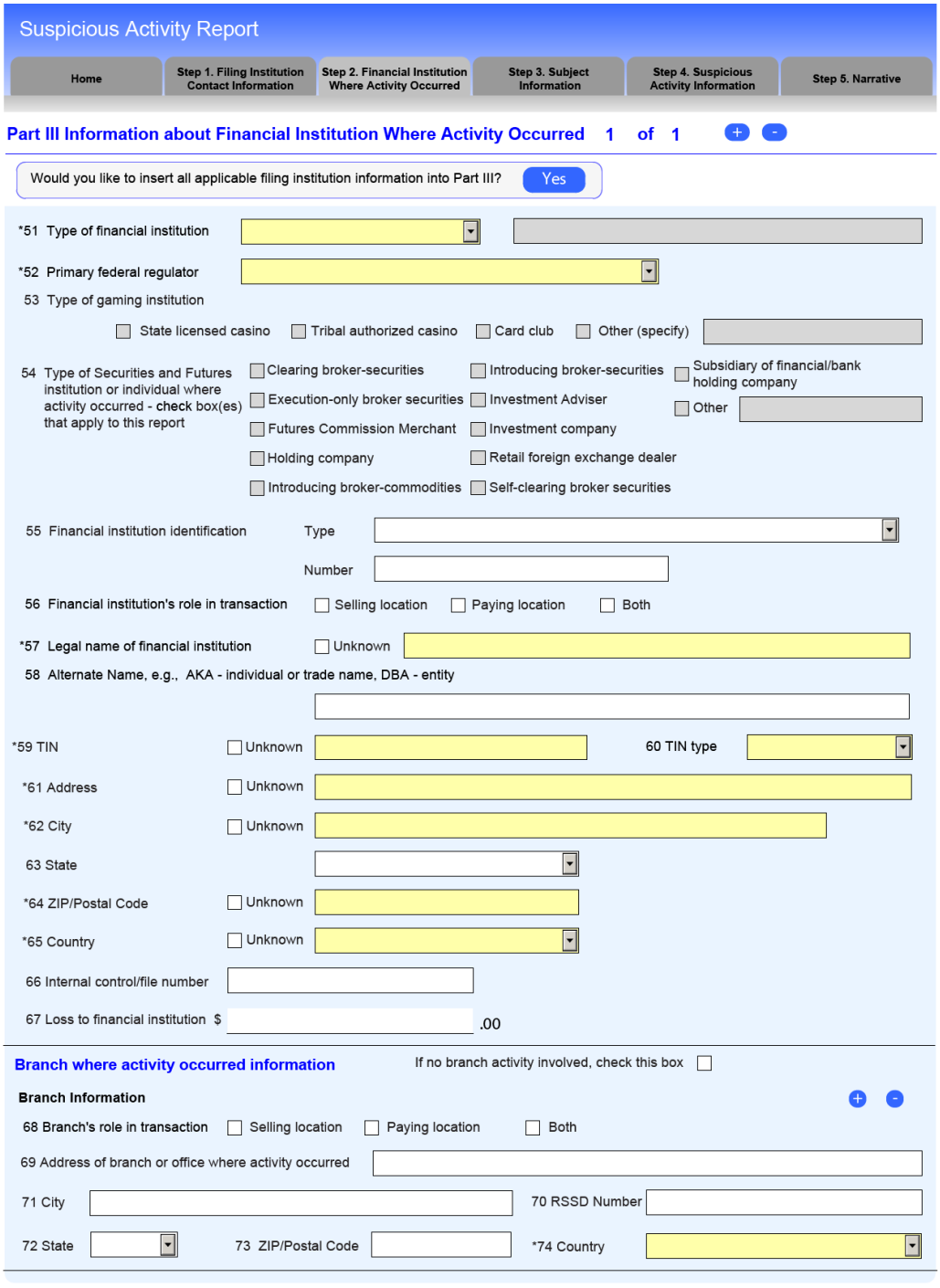
FINCEN FORM SUSPICIOUS ACTIVITY REPORT (VERSION 1.2 / 6/22/18)



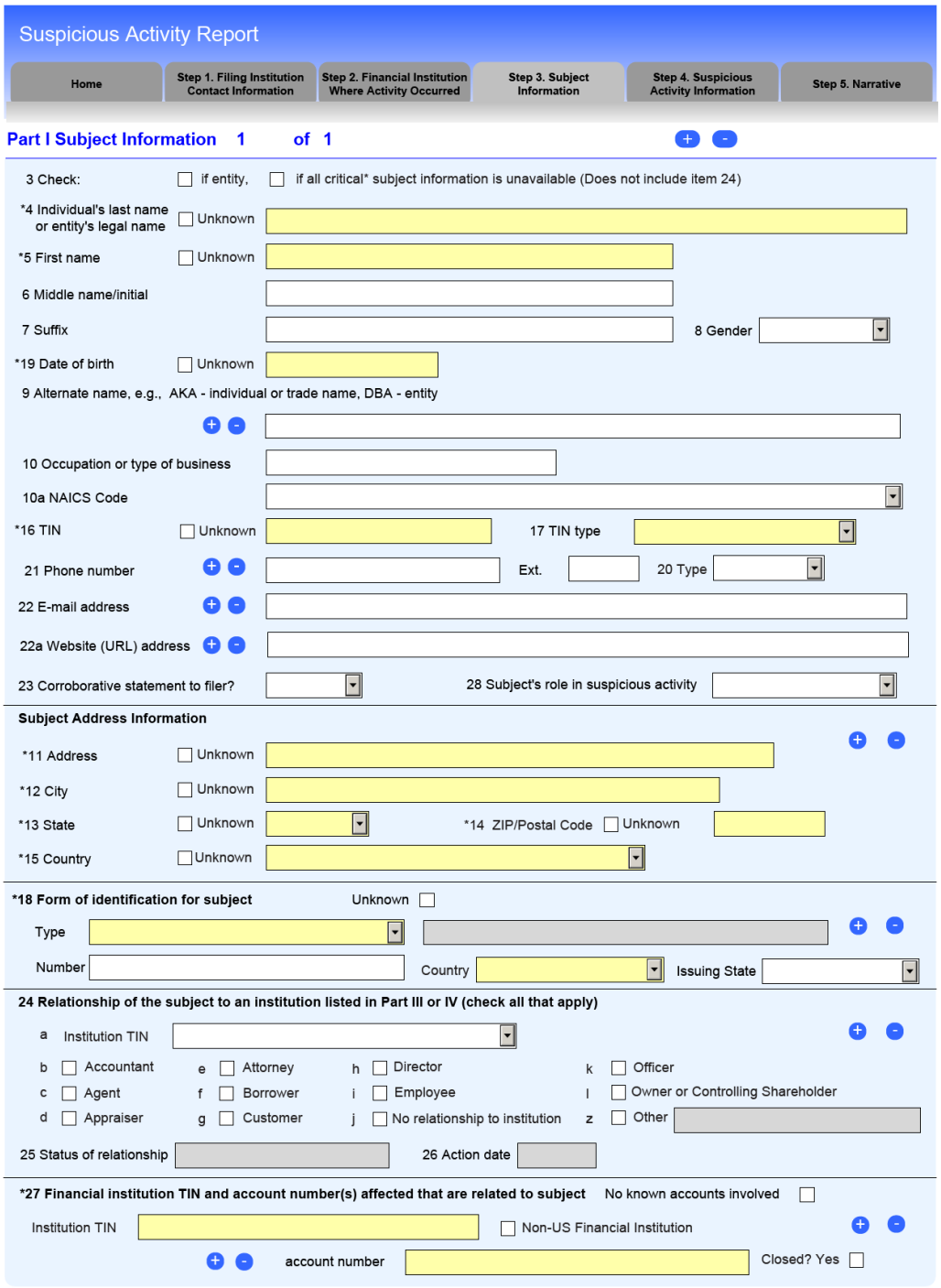
© gettechnical inc 2021



© gettechnical inc 2021



© gettechnical inc 2021



© gettechnical inc 2021

Suspicious Activity Report

Home | Step 1. Filing Institution Contact Information | Step 2. Financial Institution Where Activity Occurred | Step 3. Subject Information | Step 4. Suspicious Activity Information | Step 5. Narrative

Part II Suspicious Activity Information

*29 Amount involved in this report ☐ Amount Unknown ☐ No amount involved $ _____ .00

*30 Date or date range of suspicious activity for this report From _____ To _____

31 Cumulative amount (only applicable when "Continuing activity report" is checked in Item 1) $ _____ .00

When completing item 32 through 42, check all that apply

32 Structuring

- a ☐ Alters or cancels transaction to avoid BSA recordkeeping requirement
- b ☐ Alters or cancels transaction to avoid CTR requirement
- c ☐ Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements
- d ☐ Transaction(s) below BSA recordkeeping threshold
- e ☐ Transaction(s) below CTR threshold
- z ☐ Other

33 Terrorist Financing

- a ☐ Known or suspected terrorist/terrorist organization
- z ☐ Other

34 Fraud

- a ☐ ACH
- b ☐ Advance fee
- c ☐ Business loan
- d ☐ Check
- e ☐ Consumer loan
- f ☐ Credit/Debit card
- g ☐ Healthcare/Public or private health insurance
- h ☐ Mail
- i ☐ Mass-marketing
- j ☐ Ponzi scheme
- k ☐ Pyramid scheme
- l ☐ Securities fraud
- m ☐ Wire
- z ☐ Other

35 Gaming activities

- a ☐ Chip walking
- b ☐ Minimal gaming with large transactions
- c ☐ Suspicious use of counter checks or markers
- d ☐ Unknown source of chips
- z ☐ Other

36 Money Laundering

- a ☐ Exchange small bills for large bills or vice versa
- b ☐ Funnel account
- c ☐ Suspicion concerning the physical condition of funds
- d ☐ Suspicion concerning the source of funds
- e ☐ Suspicious designation of beneficiaries, assignees or joint owners
- f ☐ Suspicious EFT/wire transfers
- g ☐ Suspicious exchange of currencies
- h ☐ Suspicious receipt of government payments/benefits
- i ☐ Suspicious use of multiple accounts
- j ☐ Suspicious use of noncash monetary instruments
- k ☐ Suspicious use of third-party transactors (straw-man)
- l ☐ Trade Based Money Laundering/Black Market Peso Exchange
- m ☐ Transaction out of pattern for customer(s)
- z ☐ Other

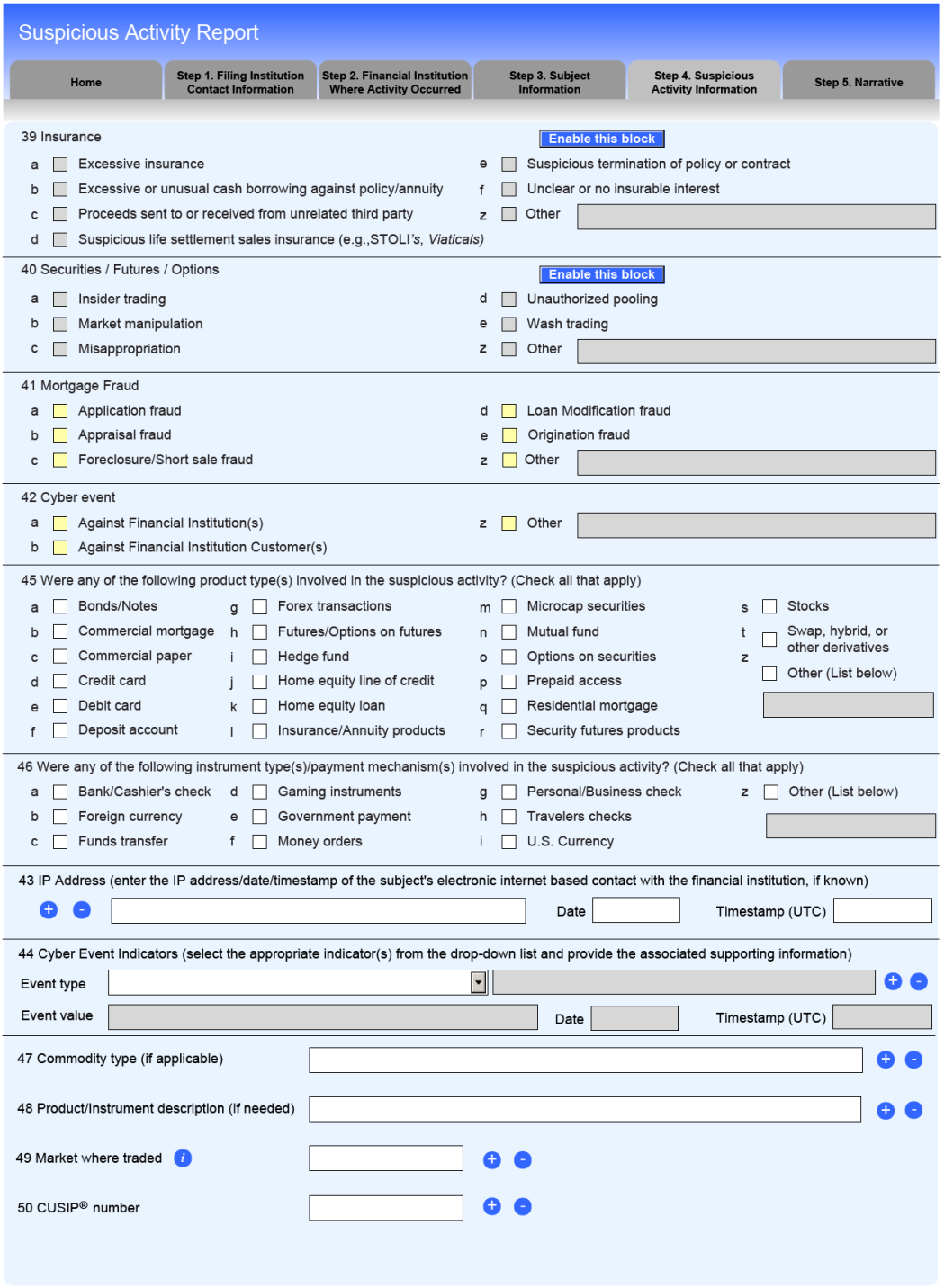
37 Identification/Documentation

- a ☐ Changes spelling or arrangement of name
- b ☐ Multiple individuals with same or similar identities
- c ☐ Provided questionable or false documentation
- d ☐ Provided questionable or false identification
- e ☐ Refused or avoided request for documentation
- f ☐ Single individual with multiple identities
- z ☐ Other

38 Other Suspicious Activities

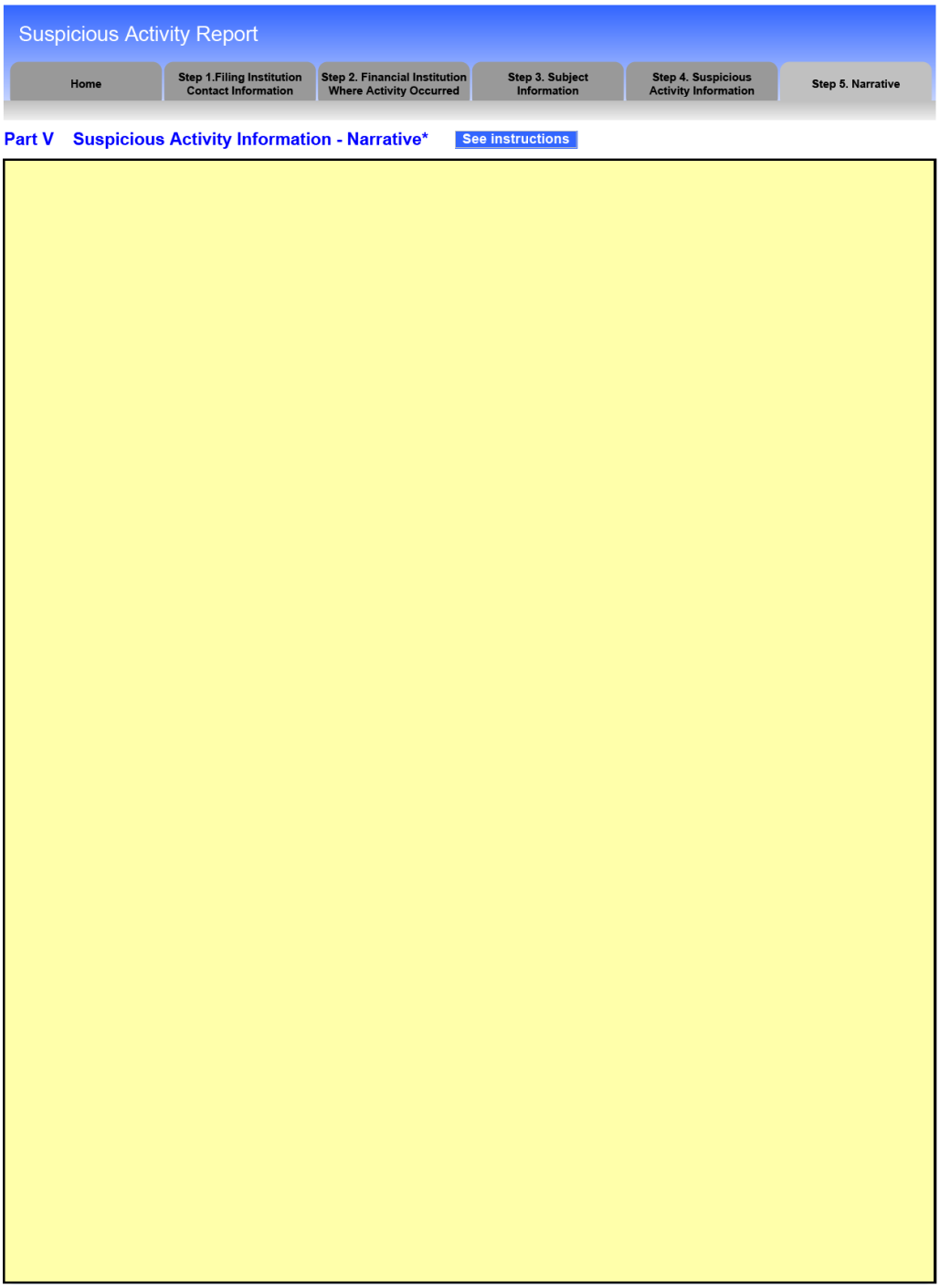
- a ☐ Account takeover
- b ☐ Bribery or gratuity
- c ☐ Counterfeit instruments
- d ☐ Elder financial exploitation
- e ☐ Embezzlement/theft/ disappearance of funds
- f ☐ Forgeries
- g ☐ Human smuggling
- h ☐ Human trafficking
- i ☐ Identity theft
- j ☐ Little or no concern for product performance penalties, fees, or tax consequences
- k ☐ Misuse of position or self-dealing
- l ☐ Suspected public/private corruption (domestic)
- m ☐ Suspected public/private corruption (foreign)
- n ☐ Suspicious use of informal value transfer system
- o ☐ Suspicious use of multiple transaction locations
- p ☐ Transaction with no apparent economic, business, or lawful purpose
- q ☐ Transaction(s) involving foreign high risk jurisdiction
- r ☐ Two or more individuals working together
- s ☐ Unlicensed or unregistered MSB
- z ☐ Other

© gettechnical inc 2021



© gettechnical inc 2021

NOTES



© gettechnical inc 2021

OVERVIEW OF FINCEN SAR CHANGES

Red text indicates new or revised information on new SAR form

➡ Points to new information

Filing institution note to FinCEN

- New text field to alert FinCEN that the FinCEN SAR is being filed in response to a current specific geographic targeting order (GTO), advisory, or other activity.

XML User Guide FinCEN SAR Jan 2018

Item 2, Filing Institution Note to FinCEN: This 50 character field is provided for the filer to alert FinCEN that this FinCEN SAR is being filed in response to a current specific geographic targeting order (GTO) or advisory or other activity. If completing for a GTO or advisory enter the GTO or advisory title/reference. Provide a brief description of the other activity. Leave Item 2 blank if the FinCEN SAR does not relate to a GTO, advisory, or other targeted activity.

© gettechnical inc 2021

Part II Suspicious Activity Information

[previously SAR 1.1 #33]
36. Money laundering
- a. Exchanges small bills for large bills or vice versa
- b. Funnel account
- c. Suspicion concerning the physical condition of funds
- d. Suspicion concerning the source of funds
- e. Suspicious designation of beneficiaries, assignees or joint owners
- f. Suspicious EFT/wire transfers
- g. Suspicious exchange of currencies
- h. Suspicious receipt of government payments/benefits
- i. Suspicious use of multiple accounts
- j. Suspicious use of noncash monetary instruments
- k. Suspicious use of third-party transactors (straw-man)
- l. Trade Based Money Laundering / Black Market Peso Exchange
- m. Transaction out of pattern for customer(s)
- z. Other (specify type of suspicious activity in space provided)

[previously SAR 1.1 #35]
38. Other suspicious activities
- a. Account takeover
- b. Bribery or gratuity
- c. Counterfeit instruments
- d. Elder financial exploitation
- e. Embezzlement/theft/disappearance of funds
- f. Forgeries
- g. Human smuggling
- h. Human trafficking
- i. Identity theft
- j. Little or no concern for product performance penalties, fees, or tax consequences
- k. Misuse of position or self-dealing
- l. Suspected public/private corruption (domestic)
- m. Suspected public/private corruption (foreign)
- n. Suspicious use of informal value transfer system
- o. Suspicious use of multiple transaction locations
- p. Transaction with no apparent economic, business, or lawful purpose
- q. Transaction(s) involving foreign high risk jurisdiction
- r. Two or more individuals working together
- s. Unlicensed or unregistered MSB
- z. Other (specify type of suspicious activity in space provided)

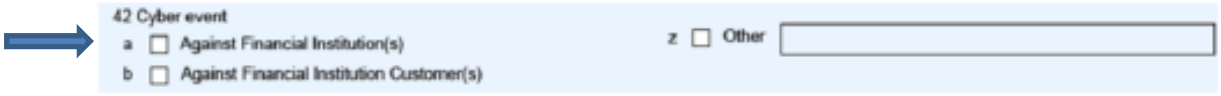
© gettechnical inc 2021

Part II Suspicious Activity Information (continued)

[SAR Form 1.1 previously #38]
41. Mortgage fraud
    a. Application fraud
    b. Appraisal fraud
    c. Foreclosure/Short sale fraud
    d. Loan modification fraud
    e. Origination fraud
    z. Other (specify type of suspicious activity in space provided)

Part II. Cyber event suspicious activity type (and associated subtypes)

- New "Cyber event" suspicious activity type category added to Part II.



XML User Guide FinCENSAR Jan 2018

Item 42, Cyber event: Complete item 42 to indicate if the cyber event was directed against the financial institution or its customer/account holder. Events against the institution may include, but not limited to, a digital denial of service (DDoS), an attempt to break (hack) into the financial institutions computer system or an attempt to take over the financial institutions "wire transfer system," the financial institutions website, a Business E-Mail Attack (BEA), etc.

Examples of cyber events against the financial institutions customer may include the takeover (or attempted takeover) of the customer's account, the sending of bogus e-mails that appear to come from the customer directing various financial transactions that do not follow the customers normal account activity, etc.

© gettechnical inc 2021

Part II Suspicious Activity Information (continued)

Part II. Date and Timestamp added to IP Address

- New text fields to accompany the IP Address field in Part II in order to record the date and/or timestamp of the first instance of the reported IP address.

[SAR Form 1.1 previously #44]
43. IP Address(es) (if available, multiples up to 99)

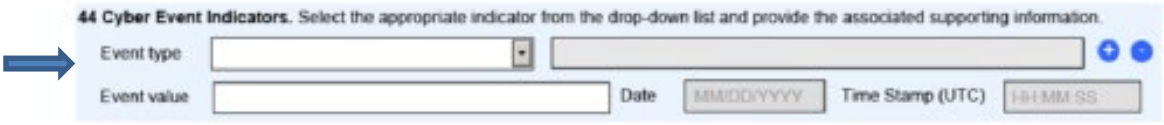
a. Date (MM/DD/YYYY)
b. Time Stamp (UTC) HH:MM:SS

Item 43 IP address: If known, enter the IP address of the subject's electronic internet based contact with the financial institution. For example, this may be the IP address used to log into the institution's online banking page or the IP address used to access an institution's mobile application. In item 43a enter the date (MM/DD/YYYY format) of the activity. In 43b enter the UTC time in (HH:MM:SS format) of the first instance of the reported IP address. Select the (+) sign to report multiple IP address, date and time information. IP address information must be explained in the FinCEN SAR Part V narrative. Batch filers will use the date format YYYYMMDD.

NOTE: If reporting an IP address in connection with a cyber-event, complete item 44.

Part II. New Cyber Event Indicators

- New category of fields to record up to 99 cyber events associated with the suspicious activity in Part II, including the event value (and date and timestamp, if applicable).



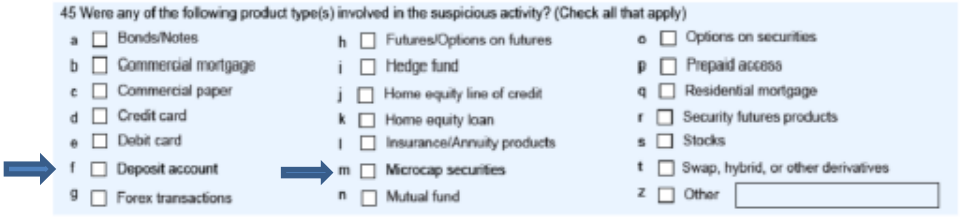
XML User Guide FinCENSAR Jan 2018

Item 44 Cyber-event indicator: Enter the cyber-event indicator by selecting the appropriate indicator from the dropdown list provided and enter the supporting information in the associated text field (an indicator not listed may be entered in the "z" Other text fields. Select the (+) sign to report multiple event indicators. Each cyber-event indicator and its associated text field is limited to 99 entries. Cyber-event indicator information must be explained in the BFinCEN SAR Part V narrative. See General Instruction 13 for additional information on reporting cyber-related events.

© gettechnical inc 2021

Part II. Updated selections associated with suspicious activity product type(s)

- New type selections associated with the product type(s) involved in the suspicious activity in Part II:
  - f. Deposit accounts
  - m. Microcap securities.



[SAR Form 1.1 previously #39]

45. Were any of the following product type(s) involved in the suspicious activity? Check all that apply:

a. Bonds/Notes
b. Commercial mortgage
c. Commercial paper
d. Credit card
e. Debit card
f. Deposit account
g. Forex transactions
h. Futures/Options on futures
i. Hedge fund
j. Home equity line of credit
k. Home equity loan
l. Insurance/Annuity products
m. Microcap securities
n. Mutual fund
o. Options on securities
p. Prepaid access
q. Residential mortgage
r. Security futures products
s. Stocks
t. Swap, hybrid or other derivative

z. Other (specify type in space provided)

Item 45 Product types involved in suspicious activity: Check all Item 45 boxes that apply to record the product type(s) involved in the suspicious activity. Option 45f 'Forex transactions" includes all foreign exchange transactions both on and off-exchange, including futures and options on foreign exchange. Option 45g "Futures/Options on futures" includes futures and options on any "commodity," as that term is defined in Section 1a(4) of the Commodity Exchange Act, including broad-based security indexes. Option 45s "Swap, hybrid or other derivative" includes all derivatives not included above including those traded over-the-counter and off-exchange. If the product type is not covered by options 45a through 45s, check box 45z "Other (list below)" and enter a brief description in the associated text field. If necessary provide a more detailed product type (such as commodity futures contracts, options on commodity futures contracts, commodity options, and OTC agricultural trade options) in Item 48 "Product/instrument description" or in Part V. If there are multiple product types not covered by Item 45, record one in Item 45z "Other (List below)" and all others in Part V.

© gettechnical inc 2021

Part III/IV. Updated subtypes associated with Securities and Futures institution

- New subtype selections associated with the type of securities and futures institution in Part III (Financial institution where activity occurred) and Part IV (Filing institution).
  - Adds Execution-only broker securities
  - Adds Self-clearing broker securities

[SAR Form 1.1 previously #83]

XML User Guide FinCENSAR Jan 2018

80 Type of Securities and Futures institution or individual filing this report - check the boxes of all types that apply to this report.

a. Clearing broker - securities
b. CPO/CTA
c. Execution-only broker securities
d. Futures commission merchant
e. Holding company
f. Introducing broker - commodities
g. Introducing broker - securities
h. Investment adviser
i. Investment company
j. Retail foreign exchange dealer
k. Self-clearing broker-securities
l. SRO Futures
m. SRO Securities
n. Subsidiary of financial/bank holding company
z. Other (specify type of institution or individual in space provided)

Item 80 - Securities and futures type: If option 80e "Securities/Futures" was selected, check all boxes that apply to indicate the type of securities and futures institution that is filing the FinCEN SAR. If none of options 80a through 80nl apply, check box 80z "Other" and record a brief description of the type in the associated text field. If necessary, include a more-detailed description in Part V.

© gettechnical inc 2021

[SAR Form 1.1 previously #50]

XML User Guide FinCENSAR Jan 2018

54. If item 51e is checked, indicate type of Securities and Futures institution or individual where activity occurred - check the boxes of all types that apply to this report.

a. Clearing broker – securities
b. Execution-only broker securities
c. Futures commission merchant
d. Holding company
e. Introducing broker - commodities
f. Introducing broker - securities
g. Investment adviser
h. Investment company
i. Retail foreign exchange dealer
j. Self-clearing broker-securities
k. Subsidiary of financial/bank holding company
z. Other (specify type of institution or individual in space provided)

Item 54 Securities and futures type: If option 51e was checked indicating the financial institution is part of the securities and futures industries, check all boxes that apply to the reported suspicious activity. If none of options 54a through 54k apply, check box 54z "Other" and record a brief description of the type in the associated text field. Examples of this are commodity pool operator or commodity trading adviser. If necessary, include a more-detailed description in Part V.

© gettechnical inc 2021

NOTES

© gettechnical inc 2021

FILINGS, CORRECTED, CONTINUING, AMENDED AND JOINT FILINGS

© gettechnical inc 2021

FILING REPORTS:

This form should be E-filed through the Financial Crime Enforcement Network (FinCEN) BSA E-Filing System. Go to http://bsaefiling.fincen.treas.gov to register if not already registered. Financial institutions that file reports individually will use FinCEN's discrete Bank Secrecy Act Suspicious Activity Report (BSA SAR) to file their reports. Financial institutions that use batch filing or system-to-system filing to transmit multiple reports must transmit files that conform to the requirements of FinCEN's "General Specifications for Electronic Filing of Bank Secrecy Act (BSA) Reports" (General Specifications) and "BSA Electronic Filing Requirements for the Bank Secrecy Act Suspicious Activity Report (BSA SAR)" (Electronic Filing Requirements).

Complete each BSA SAR by providing as much information as possible. Although all items should be completed fully and accurately, items marked with an asterisk (*) must be completed. Filers must follow the electronic filing instructions for these items by providing the required data or, if instructions permit, by checking the box "a. Unk" to indicate that the required data was unknown or not applicable. These instructions supersede all prior SAR instructions and FinCEN guidance on use of special responses in SAR items when the data is unknown or not available in an electronic filing. Therefore, the use of special responses such as "UNKNOWN," "NONE," "NOT APPLICABLE," or "XX" and their variants is prohibited in the BSA SAR.

NOTE: Throughout these instructions the phrase "check box" and similar wording is used to denote checking an appropriate box in certain data items on the discrete BSA SAR. This is deemed equivalent to instructions in the Electronic Filing Requirements to enter appropriate codes in the same data items in transmission files. For example, the requirement to check box 1a "Initial report" in the discrete BSA SAR is the equivalent of entering code "A" in "Type of Filing" in the Electronic Filing Requirements Suspicious Activity Information (3A) Record. In some discrete BSA SAR data items check boxes have been replaced by drop-down lists.

NOTE: Throughout these instructions there are requirements to complete items multiple times in a discrete BSA SAR if the filer has multiple entries for that item. This is deemed equivalent to completing multiple records for that item in the Electronic Filing Requirements. For example, these instructions direct filers to complete multiple Item 6 "Alternate name" fields if the filer has knowledge of multiple alternate names for a subject. This is equivalent to a batch filer completing multiple Subject Alternative Name (4D) Records for the same subject.

© gettechnical inc 2021

CORRECTED/AMENDED REPORTS

A corrected report on a previously-filed BSA SAR must be filed whenever errors are discovered in the data reported in that BSA SAR. An amended report must be filed on a previously-filed BSA SAR whenever new data about a reported suspicious activity is discovered and circumstances will not justify filing a continuing report (see General Instruction 4). Both corrected and amended reports must be completed in their entirety, with the necessary corrections or amendments made to the data. In both cases box 1b "Correct/Amend prior report" must be checked. If known, the prior report's Document Control Number (DCN), BSA Identifier (BSAI), or reporting financial institution file number must be entered in field 1e. All corrections or amendments must be described completely at the beginning of the Part V Suspicious Activity Information – Narrative section. If a BSA SAR is filed to correct or amend a prior SAR version, the BSA SAR must be completed in its entirety. This includes BSA SAR items that apply to the suspicious activity but were not present on the prior SAR version.

© gettechnical inc 2021

CONTINUING REPORTS:

A continuing report should be filed on suspicious activity that continues after an initial BSA SAR is filed. Continuing reports should be filed at least every 90 days until the suspicious activity ceases. Continuing reports must be completed in their entirety, including the information about all subjects involved in the suspicious activity and all financial institutions where the activity occurred. The continuing report Part V narrative should include all details of the suspicious activity for the 90-day period encompassed by the report, and only such data from prior reports as is necessary to understand the activity. Do not reproduce the narratives from prior reports in the continuing report. Provide both the dollar amount involved in the suspicious activity for the 90-day period in Item 26 and the cumulative dollar amount for the current and all prior related reports in Item 28. If continuing losses are involved for any financial institution recorded in Part III, record the 90-day loss in Item 63 and the cumulative loss in Part V.

© gettechnical inc 2021

1. Definition

A BSA SAR may be jointly filed when two or more distinct financial institutions collaborate in filing a single BSA SAR on suspicious activity involving all of the collaborating financial institutions. Financial institutions are "distinct" for this purpose when they are different legal entities; a financial institution is not distinct from its own branches.

2. Prohibition

Joint filing of a single BSA SAR is prohibited when any of the Part I subjects of the would-be jointly filed BSA SAR have a box in Item 21 checked that identifies the subject as a director, employee, officer, or owner/controlling shareholder of the filing institution or a would-be joint filer. In that case separate BSA SARs must be filed by each institution.

3. Requirements

To be a jointly-filed BSA SAR, box 1d "Joint report" must be checked. In addition, the filing institution listed in Part IV must identify in Part V which Part III institutions are joint filers. The filing institution must include joint filer contact information in Part V, along with a description of the information provided by each joint filer.

Record joint filer information in Part III Items 47 through 63 and joint filer branch information in Part III Items 64 through 77. Filing a joint BSA SAR does not relieve joint filers of the responsibility to report information about the suspicious activity that was not included in the joint filing.

4. Permission

A filing institution cannot designate another institution as a joint filer unless the designated joint filer is aware of and approves the BSA SAR filing in its entirety. A filer that designates another institution as a joint filer without gaining that institution's agreement to the joint filing and approval of the contents of the joint filing may have committed a willful violation of the Bank Secrecy Act, if the improper designation leads to the disclosure of the SAR filing to a person not entitled to information about the filing.

5. Record Retention

Both filers and joint filers are required to keep copies of the BSA SAR and their own supporting documentation for five (5) years after the date of filing.

© gettechnical inc 2021

Permission from Joint Filing Financial Institution

Our financial institution has been provided a copy of the SAR and gives our permission to the filing as a Joint filing institution.

Date_____
Document number or name_____

Name of Joint filing institution _____
Name of BSA Officer_____

_____
Signature of BSA Officer

© gettechnical inc 2021

Joint Filing Institutions

SAR File Name	Joint Institutions	Permission Obtained	314 B Checked	Copy of SAR delivered to Joint filer
Smith 05152012	ABC Financial Institution	Yes	Yes	05052012

© gettechnical inc 2021

NOTES

© gettechnical inc 2021

INFORMATION ON SUBJECTS

© gettechnical inc 2021

Addresses: For addresses in the U.S., Canada, or Mexico enter the permanent street address, city, two or three letter state/territory/province code, ZIP Code or foreign postal code, and two letter country code for the individual or entity recorded in Part I, Part III, or Part IV. Provide the apartment number or suite number, if known, following the street address. A non-location address such as a post office box or rural route number should be used only if no other street address information is available. ZIP Codes must be five or nine digits. ZIP Codes and foreign postal codes must be entered without formatting or special characters such as spaces or hyphens. For example, the ZIP Code 12354-6120 would be entered as 123546120.

The foreign postal code HKW 702 would be entered HKW702. For other foreign addresses enter the street address, city, postal code, and two letter country code or address equivalent. If a foreign address contains other address information that does not conform to the BSA SAR address format, record equivalent address information in the BSA SAR address items and the full address in Part V. Complete any address item that is known, even if the complete address is unknown. No abbreviations are permitted in city names, which must be completely spelled out.

A U.S. city name must match the city name used by the U.S. Postal Service for the associated state and ZIP Code. For U.S. address use only the authorized U.S. Postal Service state, territory, or military address abbreviations found at https://www.usps.com/ship/official-abbreviations.htm.

For Canadian provinces and territories use the Canada Post Corporation codes found at http://www.canadapost.ca/tools/pg/manual/PGaddress-e.asp#1380608. For Mexican states and territories use the ISO 3166-2 three-letter codes found at http://www.commondatahub.com/live/geography/state_province_region/iso_3166_2_state_codes

For all countries use the ISO 3166-1 two-letter country codes found at http://www.iso.org/iso/country_names_and_code_elements. Additional information about ISO 3166 codes can be found on the BSA E-Filing Program website. Note: The ISO 3166-1 country list includes entries for all U.S. territories. Do not use these U.S. territory entries, which match the U.S. Postal Service abbreviations required in state fields, in any country field.

Telephone Numbers: Record all telephone numbers, both foreign and domestic, as a single number string without formatting or special characters such as parentheses or hyphens. For example, a number in the format (NNN) NNN-NNNN would be recorded as NNNNNNNNNN. Indicate the type of telephone number provided (home, work, mobile, or fax) by checking the appropriate box. Provide the telephone extension number if known. Telephone numbers that are part of the North American Numbering Plan used by the U.S., Canada, many Caribbean countries, and current/former U.S. Pacific island protectorates must consist of an area code and seven-digit telephone number. Other foreign telephone numbers should include the country number code. If only a partial telephone number is known record that number in the phone number item and explain in Part V that the entry is a partial number.

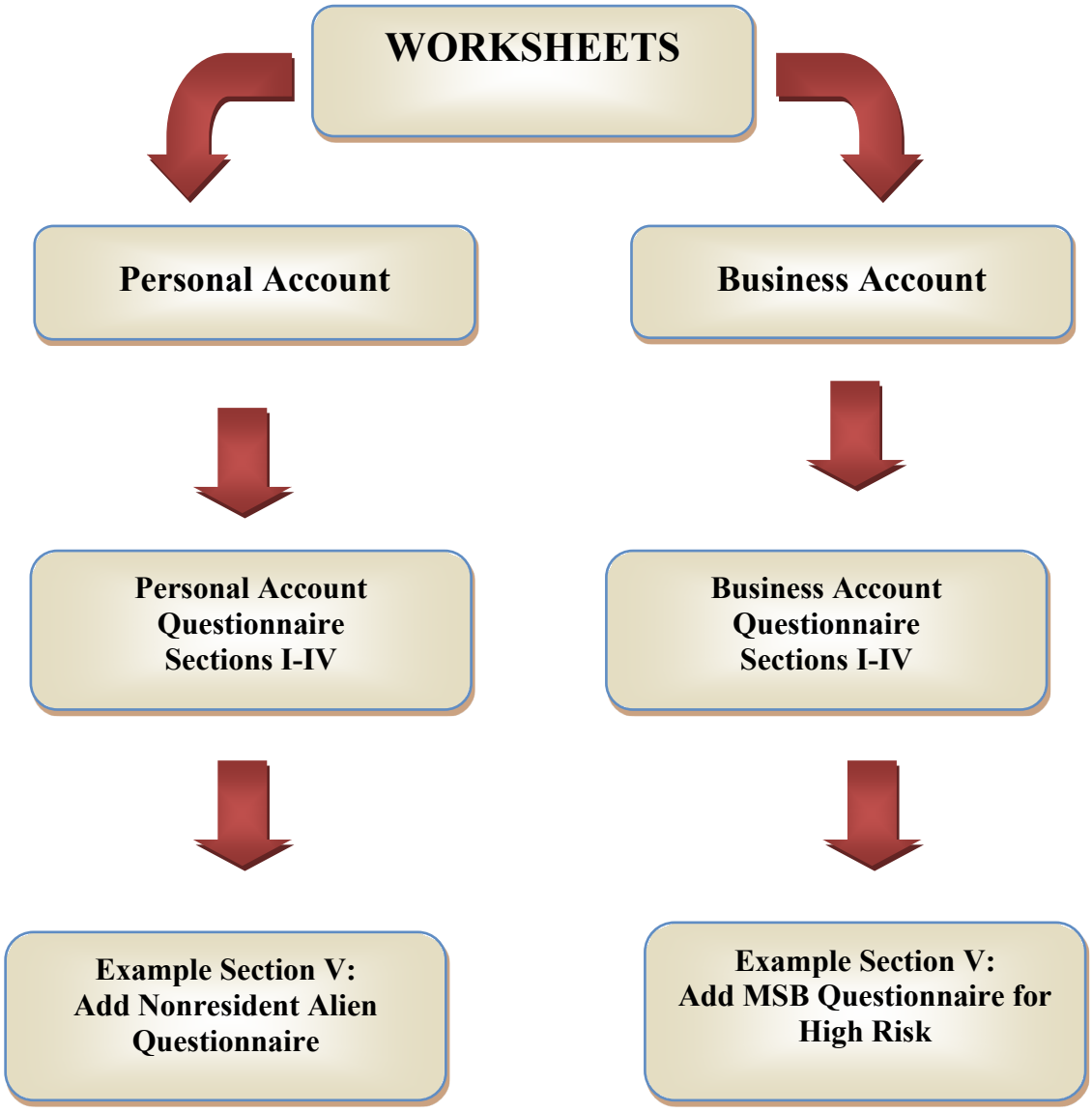
Identifying Numbers: Enter all identifying numbers as a single text string without formatting or special characters such as hyphens or periods. An identifying number in the format NNN-NN-

© gettechnical inc 2021

NNNN would be entered as NNNNNNNNN. Such numbers include alien registration, CRD, CUSIP®, driver's license, state identification, EIN, IARD, ITIN, passport, RSSD, SEC ID, and SSN.

Monetary Amounts: Record all monetary amounts in U.S. Dollars rounded up to the next whole dollar. The amount $5,265.25 would be recorded as $5,266. If the amount involves a foreign currency, record the currency name, amount, and country of origin in Part V. When converting a foreign currency to U.S. Dollars use an exchange rate for the date or dates the foreign currency was involved in the suspicious activity.

© gettechnical inc 2021



© gettechnical inc 2021

FORM: CONSUMER PROFILE

Check address against USPS

gettechnical
EDUCATION FOR FINANCIAL INSTITUTIONS

Date: _____

CIF: _____

Account Number: _____

Bank Employee:

_____

CONSUMER PROFILE

What brought you to the bank today?

❑ Open Account ❑ Gather Information ❑ Other _____

If it is to open an account, what type of account?

❑ Checking ❑ Money Market Account ❑ Loan

❑ Savings ❑ Time Deposit (CD) ❑ Other _____

Any chance you are an existing customer of the bank? ❑ Yes or ❑ No

To get your account opened, we are going to need some information:

Name: _____

Physical Address: _____

Mailing Address: _____

Phone numbers Home: _____

Work: _____

Cell: _____

SSN or ITIN: _____

(If no SSN or ITIN, Passport or other identification number)

Occupation: _____

Email Address: _____

Household Income: _____

We will also need two forms of identification: (Attach copies. Do not photocopy or scan military ID)

Are you a US Person (US Person includes resident alien) ❑ Yes or ❑ No

If you are a nonresident alien, what country are you from?

_____

Are you an elected official? ❑ Yes or ❑ No

Now to get you in the right product, we will need to know how you plan to use this account?

❑ Household Operating Account? ❑ Savings

❑ Separate Account For Special Purpose? ❑ Other _____

1 of 3

© gettechnical inc 2021

Where are you moving the funds from?

Name of financial institution _____

How do you plan to fund this account?

❑ Cash
❑ On Us Transfer Or Check
❑ Payroll Check
❑ Government Check
❑ Cashier's Check
❑ Wire
❑ Foreign Funds

What is your expected account usage?

❑ General Personal ❑ Other: (Specify) _____

Deposits / Month (Est) _____ # Checks & Withdrawals / Month (Est) _____

$ Deposits / Month (Est) _____ $ Checks & Withdrawals / Month (Est) _____

Deposit Cash? ❑ Yes / ❑ No

If YES, estimate amount $_____ ❑ Per Month / ❑ Per Transaction

Withdraw Cash? ❑ Yes / ❑ No

If YES, estimate amount $_____ ❑ Per Month / ❑ Per Transaction

Purpose: _____

Incoming Wires? ❑ Yes / ❑ No

If YES, estimate amount $_____ Per Wire

Frequency: _____ Per Day / Week / Month (circle)

Country(ies) of Origin: _____

Purpose: _____

Outgoing Wires? ❑ Yes / ❑ No

If YES, estimate amount $_____ Per Wire

Frequency: _____ Per Day / Week / Month (circle)

Send to Country(ies) : _____

Purpose: _____

Purchase Monetary Instruments ❑ Yes / ❑ No

If YES, estimate amount $_____

Purpose: _____

ACH Deposits ❑ Yes / ❑ No

If YES, expected source of deposits: _____

ACH Debits ❑ Yes / ❑ No Online Banking ❑ Yes / ❑ No

Other Bank Services Customer Is Interested In: _____

(Loans, Cashier's Checks, etc)

© gettechnical inc 2021

Will you have your payroll/social security coming in automatically into this account? ❑ Yes or ❑ No

Now to get you in the right ownership, we will need to know how you plan to own this account?

❑ Individual ❑ Joint ❑ POD ❑ Fiduciary

If this is a Fiduciary, what type?

❑ Custodian ❑ Representative Payee

❑ Power of Attorney ❑ VA Fiduciary

Date of Profile: _____ OFAC/PEP: _____

BSA Risk Rating: _____ 3rd Party Vendor: _____

Opened by: _____

Input by: _____

Reviewed by: _____

© gettechnical inc 2021

FORM: LEGAL ENTITY PROFILE

gettechnical
EDUCATION FOR FINANCIAL INSTITUTIONS

LEGAL ENTITY PROFILE

(Check one)

❑ New Customer
❑ Existing Customer
❑ Exempt

(Check one)

❑ In Person
❑ Other _____

PART 1 Information

Name of legal entity: _____
Physical address: _____
Mailing address: _____
Phone number: _____
Email address: _____
Website: _____
Type of Legal Entity ❑ Corp ❑ LLC ❑ Partnership ❑ Sole Proprietorship ❑ Nonprofit ❑ Agent ❑ Trust ❑ Estate ❑ Other _____
NAICS: _____
What does the business do? _____
What is the expected annual revenue? _____
Where is customer currently banking? _____
What counties/ parishes does the business operate in? _____
What states does the business operate in? _____
Where are your customers located? _____
What is the purpose of the account (Operations, Payroll, etc)? _____
Which bank is the money coming from? _____

1 of 8

© gettechnical inc 2021

PART 2 Expected Account Usage

Deposits / Month (Est) _____ # Checks & Withdrawals / Month (Est) _____

$ Deposits / Month (Est) _____ $ Checks & Withdrawals / Month (Est) _____

Deposit Cash? ❑ Yes / ❑ No

If YES, estimate amount $_____ ❑ Per Month / ❑ Per Transaction

Withdraw Cash? ❑ Yes / ❑ No

If YES, estimate amount $_____ ❑ Per Month / ❑ Per Transaction

Purpose: _____

Incoming Wires? ❑ Yes / ❑ No

If YES, estimate amount $_____ Per Wire

Frequency: _____ Per Day / Week / Month (circle)

Country(ies) of Origin: _____

Purpose: _____

Outgoing Wires? ❑ Yes / ❑ No

If YES, estimate amount $_____ Per Wire

Frequency: _____ Per Day / Week / Month (circle)

Send to Country(ies) : _____

Purpose: _____

Purchase Monetary Instruments ❑ Yes / ❑ No

If YES, estimate amount $_____

Purpose: _____

Purpose: _____

ACH Deposits ❑ Yes / ❑ No

If YES, expected source of deposits: _____

ACH Debits ❑ Yes / ❑ No Online Banking ❑ Yes / ❑ No

PART 3 Types of Products Anticipated

❑ Checking ❑ MMF ❑ Business Loan

❑ Savings ❑ CD ❑ Other _____

© gettechnical inc 2021

PART 4 Specialized Business Types

Is the customer a professional service provider? ❑ Yes or ❑ No

Is this account an IOLTA account? ❑ Yes or ❑ No

Internet Gambling Questions

Does your company have any games or financial activities on its website? ❑ Yes or ❑ No

Do you provide services to companies who provide internet gambling? ❑ Yes or ❑ No

If legal in your state, provide licensing. Otherwise have company sign certification that it is not engaged in unlawful internet gambling.

MSB Questions

Does your company cash checks over $1000? ❑ Yes or ❑ No

Does your company issue cashier's checks or money orders over $1000? ❑ Yes or ❑ No

Does your company exchange currency over $1000? ❑ Yes or ❑ No

Do you transmit currency even virtual currency at any dollar amount? ❑ Yes or ❑ No

Do you provide prepaid cards? ❑ Yes or ❑ No

If so you must register as an MSB with fincen.gov

Excludes: HSA, HRAs, FSAs, closed loop under $2000, cards that are over $1000 but are not reloadable, cards that do not allow international transactions

Do you sell prepaid cards? ❑ Yes or ❑ No

If so, provide: • Copy of AML Policy • Copy of Registration with FinCEN • Previous Bank Statements.

Privately Held ATMs (Complete when customer has an ATM on premise not owned by a bank)

Does the business have any private ATM machines located on the premises? ❑ Yes or ❑ No

If so, does your business own or lease from another contractor? We will need:

- Copy of the ATM agreement with sponsoring entity
- Exact physical location(s) of the ATM(s)
- Copy of state registration (if required by state)
- Copy of three months ATM activity statements
- Description of currency servicing arrangements customer will include
- How is cash being replenished (store proceeds, armored car, etc)

Casino (Complete for Casinos and Card Clubs)

Is the customer a casino? ❑ Yes or ❑ No

If so, please provide: • Copy of AML Policy • Copy of Audit • Previous Bank Statements.

© gettechnical inc 2021

Nongovernment Organizations (Charities, nonprofit, clubs, civic organizations, campaigns)

What is the purpose of your nonprofit organization?_____

_____

Where do the donations come from?_____

_____

How is your organization structured?_____

_____

Note: some are required to register at secretary of state if so a copy of the state registration

Medical Marijuana Related Questions

Is this business a marijuana-related business? ❑ Yes or ❑ No

Type of business _____

(Example Insurance company, landlord, security systems etc.)

Approximate annual revenue _____

What percentage of your business is directly tied to marijuana business? _____%

What process do you have in place to make sure the marijuana business is licensed? _____

_____

Third Party Payment Processors

Do you process payments for another person or entity? ❑ Yes or ❑ No

- If you do, we will need a list of your merchants.
- We will need all the anticipated volume and types of transactions that you will engage in.
- We will need 3 months of your previous bank statements.

Does your third party payment processor lease space to other processors? ❑ Yes or ❑ No

What is the volume?_____

What types of transactions are processed?_____

Who are your clients?_____

How do you screen a new merchant?_____

What types of instruments are used for payments?

❑ ACH

❑ Remotely created checks

❑ Other _____

© gettechnical inc 2021

Third Party Payment Processors (cont)

What geographic regions do you cover?

❑ In state ❑ In the US

❑ In county ❑ International

How many merchants do you process for? _____

Do you rent space on your server to other payment processors?_____

Do you keep returns in a separate account?_____

What percentage of returns do you have?_____

PART 5 Documentation on Structure of the Business

Customer will provide domestic documents for business which began in this state. Foreign documentation if from another state. Customers who meet CIP documentation exemption are noted on exemption list. Obtain fictitious name when applicable. We may require ID on all signers.

Documentary verification:

- Sole Proprietorship: Government issued document, if required
- General Partnership: Partnership agreement (if any), Government issued document.
- Limited Liability Partnership: Partnership Registration, Partnership Agreement.
- Limited Partnership: Government issued document, Partnership Agreement.
- Limited Liability Company: Government issued document, Operating Agreement.
- Corporation: Government issued document, Minutes.

Nondocumentary verification:

- Third Party Verification
- Secretary of State
- Letter of Welcome

Any discrepancy in documentation and secretary of state? ❑ Yes or ❑ No

How is it being resolved?_____

_____

© gettechnical inc 2021

PART 6 Only Complete for Legal Entities Registered at Secretary of State

**See exemptions for documentation on business and exemptions for documentation on owners.*

Persons opening an account on behalf of a legal entity must provide the following information:

a. Name & Title of Person Opening Account:

_____

b. Name & Type of Legal Entity for Which the Account is Being Opened:

_____

c. The following information for each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of the legal entity listed above. Do not put entities.

1. _____ _____ ❑ Copy of ID obtained
Name Date of Birth

_____ _____
Address (Residential or Business Street Address) *Social Security Number

2. _____ _____ ❑ Copy of ID obtained
Name Date of Birth

_____ _____
Address (Residential or Business Street Address) *Social Security Number

3. _____ _____ ❑ Copy of ID obtained
Name Date of Birth

_____ _____
Address (Residential or Business Street Address) *Social Security Number

4. _____ _____ ❑ Copy of ID obtained
Name Date of Birth

_____ _____
Address (Residential or Business Street Address) *Social Security Number

(If no individual meets this definition, please write "Not Applicable.")
(Nonprofit Corporations do not have 25% owner section, only Part d.)
** If Non US Person use SSN, Passport Number or similar number.*

© gettechnical inc 2021

PART 6 Only Complete for Legal Entities Registered at Secretary of State (cont)

d. The following information for one individual with significant responsibility for managing the legal entity listed above, such as:

- An executive officer or senior manager (e.g., Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, Treasurer); or
- Any other individual who regularly performs similar functions.

If appropriate, an individual listed under section (c) above may also be listed in this section (d).

_____ _____ ❑ Copy of ID obtained

Name Date of Birth

_____ _____

Address (Residential or Business Street Address) *Social Security Number

I, _____ (name of person opening account), hereby certify, to the best of my knowledge, that the information provided above is complete and correct.

Signature: _____ *Date:* _____

** If Non US Person use SSN, Passport Number or similar number.*

Date of Profile: _____ OFAC/PEP: _____

BSA Risk Rating: _____ 3rd Party Vendor: _____

Opened by: _____

Input by: _____

Reviewed by: _____

© gettechnical inc 2021

Exemptions for documentation.
Exempt from both CIP and beneficial ownership.

- A financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator;
- Exempt person. For purposes of this section, an exempt person is:

  (1) A bank, to the extent of such bank's domestic operations;

  (2) A department or agency of the United States, of any State, or of any political subdivision of any State;

  (3) Any entity established under the laws of the United States, of any State, or of any political subdivision of any State, or under an interstate compact between two or more States, that exercises governmental authority on behalf of the United States or any such State or political subdivision;

  (4) Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stock or interests listed under the separate "NASDAQ Capital Markets Companies" heading), provided that, for purposes of this paragraph (b)(4), a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations;

Other exemptions for beneficial owners.

- (5) Any subsidiary, other than a bank, of any entity described in paragraph (b)(4) of this section (a "listed entity") that is organized under the laws of the United States or of any State and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity, provided that, for purposes of this paragraph (b)(5), a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations;
- An issuer of a class of securities registered under section 12 of the Securities Exchange Act of 1934 or that is required to file reports under section 15(d) of that Act;
- An investment company, as defined in section 3 of the Investment Company Act of 1940, that is registered with the Securities and Exchange Commission under that Act;
- An investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940, that is registered with the Securities and Exchange Commission under that Act;
- An exchange or clearing agency, as defined in section 3 of the Securities Exchange Act of 1934, that is registered under section 6 or 17A of that Act;
- Any other entity registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, each as defined in section 1a of the Commodity Exchange Act, that is registered with the Commodity Futures Trading Commission;
- A public accounting firm registered under section 102 of the Sarbanes–Oxley Act;
- A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act (12 U.S.C 1467a(n));
- A pooled investment vehicle that is operated or advised by a financial institution excluded under paragraph (e)(2) of this section;
- An insurance company that is regulated by a State;
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010;
- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
- Any legal entity only to the extent that it opens a private banking account subject to §1010.620 of this chapter.

The Legal entity customers are subject only to the control.

- A pooled investment vehicle that is operated or advised by a financial institution not excluded under paragraph (e)(2) of this section; and
- Any legal entity that is established as a nonprofit corporation or similar entity and has filed its organizational documents with the appropriate State authority as necessary.

Activity Exemptions as long as no payments to or receive from third parties.

- At the point-of-sale to provide credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of $50,000;
- To finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- To finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker;
- To finance the purchase or leasing of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

Existing Customers are not exempt from beneficial ownership if the entity is adding a new account

© gettechnical inc 2021

FORM: BSA REFERRAL

BSA Referral Form

❑ Initial Report ❑ Continued Activity - Last Report Date:_____

PART I Suspect(s) Information

Name: _____ Work Phone: _____

Address: _____ Home Phone: _____

SSN or EIN: _____ Date of Birth: _____

Passport #: _____ DL State & #: _____

PART 2 Account Information

Account Owner?

❑ Yes ❑ No If No, Explain: _____

Account Number(s):

1: _____ 2: _____

3: _____ 4: _____

PART 3 Transaction Information

Date: _____ Amount: _____

Description: _____

CTR Filed? ❑ Yes ❑ No Date: _____

Date: _____ Amount: _____

Description: _____

CTR Filed? ❑ Yes ❑ No Date: _____

Date: _____ Amount: _____

Description: _____

CTR Filed? ❑ Yes ❑ No Date: _____

1 of 5

© gettechnical inc 2021

PART 4 Suspicious Activity Discussion

Fill out any useful information regarding the transactions or incident when checking "Other".

Structuring

- ❑ Alters or cancels transaction to avoid BSA recordkeeping requirement
- ❑ Alters or cancels transaction to avoid CTR requirement
- ❑ Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements
- ❑ Transaction(s) below BSA recordkeeping threshold
- ❑ Transaction(s) below CTR threshold
- ❑ Other (specify type of suspicious activity in space provided): _____

Terrorist Financing

- ❑ Known or suspected terrorist / terrorist organization
- ❑ Other (specify type of suspicious activity in space provided): _____

Fraud

- ❑ ACH
- ❑ Advance fee
- ❑ Business loan
- ❑ Check
- ❑ Consumer Loan
- ❑ Credit / Debit Card
- ❑ Healthcare/Public or private health insurance
- ❑ Mail
- ❑ Mass-marketing
- ❑ Ponzi scheme
- ❑ Pyramid scheme
- ❑ Wire

Gaming

- ❑ Chip walking
- ❑ Minimal gaming with large transactions
- ❑ Suspicious use of counter checks or markers
- ❑ Unknown source of chips

Gaming (cont)

- ❑ Other (specify type of suspicious activity in space provided) _____

Money Laundering

- ❑ Exchanges small bills for large bills or vice versa
- ❑ Funnel Account
- ❑ Suspicion concerning the physical condition of funds
- ❑ Suspicion concerning the source of funds
- ❑ Suspicious designation of beneficiaries, assignees or joint owners
- ❑ Suspicious EFT/ Wire transfers
- ❑ Suspicious exchange of currencies
- ❑ Suspicious receipt of government payments or benefits
- ❑ Suspicious use of multiple accounts
- ❑ Suspicious use of noncash monetary instruments
- ❑ Suspicious use of third-party transactors (straw-man)
- ❑ Trade Based Money Laundering / Black Market Peso Exchange
- ❑ Transaction out of pattern for customer (s)
- ❑ Other (specify type of suspicious activity in space provided): _____

Identification / Documentation

- ❑ Changes spelling or arrangement of name
- ❑ Multiple individuals with same or similar identities
- ❑ Provided questionable or false documentation
- ❑ Refused or avoided request for documentation
- ❑ Single individual with multiple identities
- ❑ Other (specify type of suspicious activity in space provided): _____

© gettechnical inc 2021

PART 4 Suspicious Activity Discussion (cont)

Fill out any useful information regarding the transactions or incident when checking "Other".

Other Suspicious Activities

- ❑ Account takeover
- ❑ Bribery or gratuity
- ❑ Counterfeit instruments
- ❑ Elder financial exploitation
- ❑ Embezzlement, theft or disappearance of funds
- ❑ Forgeries
- ❑ Human smuggling
- ❑ Human trafficking
- ❑ Identity theft
- ❑ Little or no concern for product performance penalties, fees, or tax consequences
- ❑ Misuse of position or self-dealing
- ❑ Suspected public/ private corruption (domestic)
- ❑ Suspected public/ private corruption (foreign)
- ❑ Suspicious use of informal value transfer system
- ❑ Suspicious use of multiple transaction locations
- ❑ Transaction with no apparent economic, business, or lawful purpose
- ❑ Transaction(s) involving foreign high risk jurisdiction
- ❑ Two or more individuals working together
- ❑ Unlicensed or unregistered MSB
- ❑ Other (specify type of suspicious activity in space provided): _____

_____

Insurance

- ❑ Excessive insurance
- ❑ Excessive or unusual cash borrowing against policy/annuity
- ❑ Proceeds sent to or received from unrelated third party
- ❑ Suspicious life settlement sales insurance (e.g. STOLIs, Viaticals)
- ❑ Suspicious termination of policy or contract

Insurance (cont)

- ❑ Unclear or no insurable interest
- ❑ Other (specify type of suspicious activity in space provided): _____

_____

Securities / Futures / Options

- ❑ Insider trading
- ❑ Market manipulation
- ❑ Misappropriation
- ❑ Unauthorized pooling
- ❑ Wash Trading
- ❑ Other (specify type of suspicious activity in space provided): _____

_____

Mortgage Fraud

- ❑ Application fraud
- ❑ Appraisal fraud
- ❑ Foreclosure/Short sale fraud
- ❑ Loan modification fraud
- ❑ Origination Fraud
- ❑ Other (specify type of suspicious activity in space provided): _____

_____

Cyber event (If reporting)

- ❑ Against Financial Institution(s)
- ❑ Against Financial Institution Customer(s)
- ❑ Other (specify type of suspicious activity in space provided): _____

_____

© gettechnical inc 2021

PART 4 Suspicious Activity Discussion (cont)

Were any of the following product type(s) involved in the suspicious activity? Check all that apply

- ❑ Bonds / Notes
- ❑ Commercial mortgage
- ❑ Commercial paper
- ❑ Credit card
- ❑ Debit Card
- ❑ Deposit account
- ❑ Forex transactions
- ❑ Futures/Options on futures
- ❑ Hedge fund
- ❑ Home equity line of credit
- ❑ Home equity loan
- ❑ Insurance/Annuity products
- ❑ Microcap securities
- ❑ Mutual fund
- ❑ Options on securities
- ❑ Prepaid access
- ❑ Residential mortgage
- ❑ Security futures products
- ❑ Stocks
- ❑ Swap, hybrid or other derivative
- ❑ Other: _____

_____

Were any of the following instrument type(s)/payment mechanism(s) involved in the suspicious activity? Check all that apply

- ❑ Bank / cashier's check
- ❑ Foreign currency
- ❑ Funds transfer
- ❑ Gaming instruments
- ❑ Government payment
- ❑ Money orders
- ❑ Personal/Business check
- ❑ Travelers checks
- ❑ U.S. Currency
- ❑ Other: _____

_____

Other Commentary

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

© gettechnical inc 2021

PART 5 Preparer Information

Name: _____

Work Phone: _____ Date: _____

Print Name: _____ Signature: _____

PART 6 Reviewer Information

Name: _____

Work Phone: _____ Date: _____

SAR Filed? ❑ Yes ❑ No Date: _____

Print Name: _____ Signature: _____

Note: documentation or additional information may be attached to the submission to the BSA Officer.

© gettechnical inc 2021

FORM: BSA REFERRAL FOR MORTGAGES

BSA Referral For Mortgages

❑ Initial Report ❑ Continued Activity - Last Report Date:_____

PART I Suspect(s) Information

Name: _____ Work Phone: _____

Address: _____ Home Phone: _____

SSN or EIN: _____ Date of Birth: _____

Passport #: _____ DL State & #: _____

PART 2 Account Information

Account Owner?

❑ Yes ❑ No If No, Explain: _____

Account Number(s):

1: _____ 2: _____

3: _____ 4: _____

PART 3 Transaction Information

Date: _____ Amount: _____

Description: _____

CTR Filed? ❑ Yes ❑ No Date: _____

Date: _____ Amount: _____

Description: _____

CTR Filed? ❑ Yes ❑ No Date: _____

Date: _____ Amount: _____

Description: _____

CTR Filed? ❑ Yes ❑ No Date: _____

1 of 3

© gettechnical inc 2021

PART 4 Suspicious Activity Discussion

Report Suspicious Activity even if the bank does not take a loss

Type of crime suspected

- ❑ Occupancy fraud
- ❑ Income fraud
- ❑ Appraisal fraud
- ❑ Employment fraud
- ❑ Liability fraud
- ❑ Debt elimination schemes
- ❑ Foreclosure rescue scams
- ❑ Social Security Number (SSN) Fraud and other Identity Theft
- ❑ Home Equity Conversion Mortgage (HECM)
- ❑ Reverse Mortgage scheme

Check the boxes of any of the following red flags involved

❑ Borrower/buyer submits invalid documents in order to cancel his or her mortgage obligations or to pay off his or her loan balance(s).

❑ Same notary public and/or other "authorized representative" preparing , signing, and sending packages of nearly identical debt elimination documents for multiple borrowers with outstanding mortgage balances.

❑ Same notary public and/or other "authorized representative" working with and/or receiving payments from unusually large numbers of borrowers.

❑ Falsification of certified checks, cashier's checks or "non-cash item checks" drawn against a borrower/buyer's account , rather than from the account of a financial institution.

❑ Borrower / buyer applies for a loan for a "primary residence "but does not reside in the new primary residence as indicated on the loan application; other individuals occupy the borrower or buyer's new primary residence indicating the property is being used as a secondary residence or income-generating property .

❑ Borrower/buyer of a younger age purchases his or her "primary residence" in a senior citizen residential development.

❑ Borrower/buyer requests refinancing for "primary residence" when public and personal documents indicate that the borrower / buyer resides somewhere other than the address on the loan application.

❑ Language included in a short sale contract indicates the property could be resold promptly. This possibly illegal "flipping" may occur regard less of whether the Federal Housing Administration (FHA) has re-enacted or waived its arms-length resale regulations to FHA buyers.

❑ Low appraisal values, non-arms length relationships between short sale buyers and sellers, or previous fraudulent sale attempts in short-sale transactions.

❑ Agent of the buyer and/or seller in mortgage transaction is unlicensed.

❑ Past misrepresentations made by borrower or buyer in attempts to secure funding, property, refinance, and or shorts-sales.

❑ Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information.

© gettechnical inc 2021

PART 4 Suspicious Activity Discussion (cont)

❑ Apparent resubmission of rejected loan application with key borrower / buyer details changed or modified from individual borrower to company/corporation. This activity may identify the same person attempting to secure a loan fraudulently through a straw-borrower or non-existent person.

❑ Borrower / buyer attempts to structure currency deposits / withdrawals, or otherwise to hide or disguise the true value of assets, in order to qualify for loan modification programs intended for those homeowners in financial distress.

❑ Request from third party affiliates on behalf of distressed homeowners to pay fees in advance of the homeowner receiving mortgage counseling, foreclosure avoidance, a loan modification, or other related services.

❑ Third party solicitation of distressed homeowners for purported mortgage counseling, foreclosure avoidance, loan modification, or other related services.These third parties may also claim to be associated with legitimate mortgage lenders, the U.S. government , or a U.S. government program.

❑ Other: _____

_____

_____

_____

PART 5 Preparer Information

Name: _____

Work Phone: _____ Date: _____

Print Name: _____ Signature: _____

PART 6 Reviewer Information

Name: _____

Work Phone: _____ Date: _____

SAR Filed? ❑ Yes ❑ No Date: _____

Print Name: _____ Signature: _____

Note: documentation or additional information may be attached to the submission to the BSA Officer.

© gettechnical inc 2021

NOTES

© gettechnical inc 2021

THE NARRATIVE

© gettechnical inc 2021

THE NARRATIVE

The narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators.

1. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion.

2. This description should encompass the data provided in Parts I through III, but should include any other information necessary to explain the nature and circumstances of the suspicious activity.

3. Filers should provide any information the filers believe necessary to better enable investigators to understand the reported suspicious activity.

4. Narratives must be completed in English.

© gettechnical inc 2021

Filers should use the following checklist as a guide for preparing the narrative:

Checklist requirement	Your narrative:
If this report is a corrected or amended report, complete the report in its entirety with whatever corrections or amendments were required. Describe the corrections or amendments at the beginning of the narrative.	
If this report is a continuing report, describe the circumstances surrounding the suspicious activity for the 90-day period encompassing the report. Include information from prior BSA SAR narratives only when it is necessary for an understanding of the nature and circumstances of the suspicious activity. Never include the entire narratives of the prior BSA SARs.	
If any item in the report was insufficient for recording all item data held by the filer, record the additional data referenced by item number in the narrative. Information provided in other sections of the BSA SAR need not be repeated in the narrative unless necessary to provide a clear and complete description of the suspicious activity.	
Describe the conduct or transaction(s) that caused suspicion. If appropriate, this description should be chronological when the activity involves multiple instances or encompasses more than one day.	
Explain whether any transaction(s) involved were completed or only attempted.	
Explain who benefited and how they benefited, financially or otherwise, from the activity.	
Describe all supporting documentation and retain the documentation for five years. DO NOT include supporting documentation with the BSA SAR. (See General Instruction 6.)	
If the BSA SAR is jointly-filed, name all joint filers and describe the nature of supporting document held by the joint filers. Provide the contact office name and	

© gettechnical inc 2021

telephone number for each joint filer.	
Describe and retain any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others.	
Describe and retain any admission or explanation of the activity or transaction(s) provided by the subject(s), witness(s), or other person(s), including to whom and when it was given.	
Indicate where the suspicious activity took place, e.g. branch, cage, gaming pit, agent location, etc.	
Indicate whether the suspicious activity is an isolated incident or related to other activity.	
Indicate whether any U.S. or foreign currency or other negotiable instruments were involved. If foreign currency or other foreign instruments, provide the foreign amount, currency name, and country of origin.	
Indicate if there is any litigation related to the activity by specifying the name of the litigation and court where the action is pending.	
Describe the nature of losses and recoveries related to the suspicious activity, including aggregated losses and recoveries in continuing activity.	
Identify the names of financial institutions associated with account numbers when the financial institution TINs were unknown.	
If the subject is a foreign national provide all available information on the subject's passport(s), visa(s), and other identification. Include identifying data such as issuing date, country, document numbers, issuing authority, and nationality.	

© gettechnical inc 2021

If the suspicious activity involves transfers of funds to or from a foreign country or currency exchanges involving foreign currencies, identify the foreign currency, country of issue, and the source or destination of the funds.	
If a subject involved in the suspicious activity has an insider relationship with a financial institution, describe the subject's position with the financial institution and how that position related to the suspicious activity.	
Recommend any further investigation that might assist law enforcement authorities.	
Indicate if any information was excluded from this report and explain the nature of the excluded information and the reason(s) for exclusion.	
Provide information on the victims of the suspicious activity only when it is necessary for a complete understanding of the activity. DO NOT record victim information in a Part I Subject Information record.	
Provide information about the financial institution's business policies and practices only if it is necessary for a complete understanding of the suspicious activity. DO NOT include legal disclaimers in the narrative.	
Add Attachment: Attach an MS Excel-compatible spreadsheet with a maximum size of 1 megabyte by clicking the "Add Attachment" button on the discrete BSA SAR header page and following the instructions provided. Please see Attachment E – Batch Attachments for additional information.	

© gettechnical inc 2021

SPREADSHEET

Customer	Account	Checks	Payee	Drawer	Amount	Loss

© gettechnical inc 2021

WHEN TO FILE AND WHEN TO NOT FILE

© gettechnical inc 2021

BSA SAR FILING INSTRUCTIONS:

1. Who Must File: Certain financial intuitions operating in the United States shall file with FinCEN, to the extent and in the manner required by 31 CFR Chapter X and 12 CFR §§ 21.11, 208.62, 353.3, and 748.1, a report of any suspicious transaction relevant to a possible violation of law or regulation. The following financial institutions are required to file a BSA SAR: Banks (31 CFR §1020.320); Casinos and Card Clubs (31 CFR § 1021.320); Money Services Businesses (31 CFR § 1022.320); Brokers or Dealers in Securities (31 CFR § 1023.320); Mutual Funds (31 CFR § 1024.320); Insurance Companies (31 CFR § 1025.320); and Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR § 1026.320).

2. Filing Deadlines: A BSA SAR shall be filed no later than 30 calendar days after the date of the initial detection by the reporting financial institution of facts that may constitute a basis for filing a report. If no suspect is identified on the date of such initial detection, a financial institution may delay filing a BSA SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the financial institution shall immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a BSA SAR. Financial institutions wishing voluntarily to report suspicious transactions that may relate to terrorist activity may call FinCEN's Financial Institutions Hotline at 1-866-556-3974 in addition to filing timely a BSA SAR.

3. Filing Requirements for Financial Institutions: A financial institution must report any transaction that requires reporting under the terms of 31 CFR Chapter X if the transaction is conducted or attempted by, at, or through the financial institution and involves or aggregates at least $5,000 ($2,000 for money services businesses, except as provided in Section 6 of this document) and the financial institution knows, suspects, or has reason to suspect that the transaction or pattern of transactions of which the transaction is a part:

• Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

• Is designed, whether through structuring or other means, to evade any requirement of 31 CFR Chapter X or any other regulation promulgated under the Bank Secrecy Act, Public Law 91-508, as amended, codified at 12 U.S.C 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5332;

• Has no business or apparent lawful purpose or is not the sort in which the particular customer

© gettechnical inc 2021

would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or

• Involves the use of the financial institution to facilitate criminal activity.

4. Additional Filing Instructions for Banks: In addition to the above requirements, a bank (as defined in 31 CFR § 1010.100) must file a BSA SAR for activity (as required by 31 CFR § 1020.320 and 12 CFR §§ 21.11, 208.62, 353.3, and 748.1) involving:

• **Insider abuse involving any amount.** Whenever the bank detects any known or suspected Federal criminal violations, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.

• **Violations aggregating $5,000 or more where a suspect can be identified.** Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $5,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an “alias,” then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers’ licenses or social security numbers, addresses and telephone numbers, must be reported.

• **Violations aggregating $25,000 or more regardless of a potential suspect.** Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $25,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

5. Voluntary BSA SAR Filings: Financial institutions may also file with FinCEN a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR Chapter X. A voluntary filing does not relieve a financial institution from the responsibility of complying with any other reporting requirements imposed by the SEC, the CFTC, a self-regulatory organization (SRO) (as defined in section 3(a)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78c (a)(26)), or any Registered Futures Association (RFA) or Registered Entity (RE) (as these terms are defined in the Commodity Exchange Act, 7 U.S.C. 21 and 7 U.S.C. 1a(29)).

© gettechnical inc 2021

6. Exceptions: The following are exceptions to the BSA SAR reporting requirements:

• A bank, casino, broker or dealer in securities (BD), futures commission merchant (FCM), or introducing broker in commodities (IB-C) is not required to file a BSA SAR for a robbery or burglary committed or attempted against the financial institution when the robbery or burglary is reported to appropriate law enforcement authorities.

• A BSA SAR is not required to be filed for lost, missing, counterfeit, or stolen securities that are reported pursuant to the requirements of 17 CFR § 240.17f-1.

• A BD is not required to file a BSA SAR on violations of any of the Federal securities laws or the rules of a SRO by the BD or any of its officers, directors, employees or other registered representatives, other than a violation of 17 CFR § 240.17a-8 or 17 CFR § 405.4, so long as such violation is appropriately reported to the SEC or an SRO.

• An FCM or an IB-C, or any of its officers, directors, employees or associated persons, is not required to file a BSA SAR for a violation of the Commodity Exchange Act (7 U.S.C. 1 *et seq.)*, the regulations of the CFTC (17 CFR Chapter 1), or the rules of any RFA or RE (as those terms are defined in the Commodity Exchange Act, 7 U.S.C. 21 and 7 U.S.C. 1a(29)), as long as such violation is appropriately reported to the CFTC, an RFA, or RE. This exception does not apply to violations of 17 CFR § 42.2.

• An insurance company is not required to report the submission to it of false or fraudulent information to obtain a policy or make a claim, unless the company has reason to believe that that the false or fraudulent submission relates to money laundering or terrorist financing.

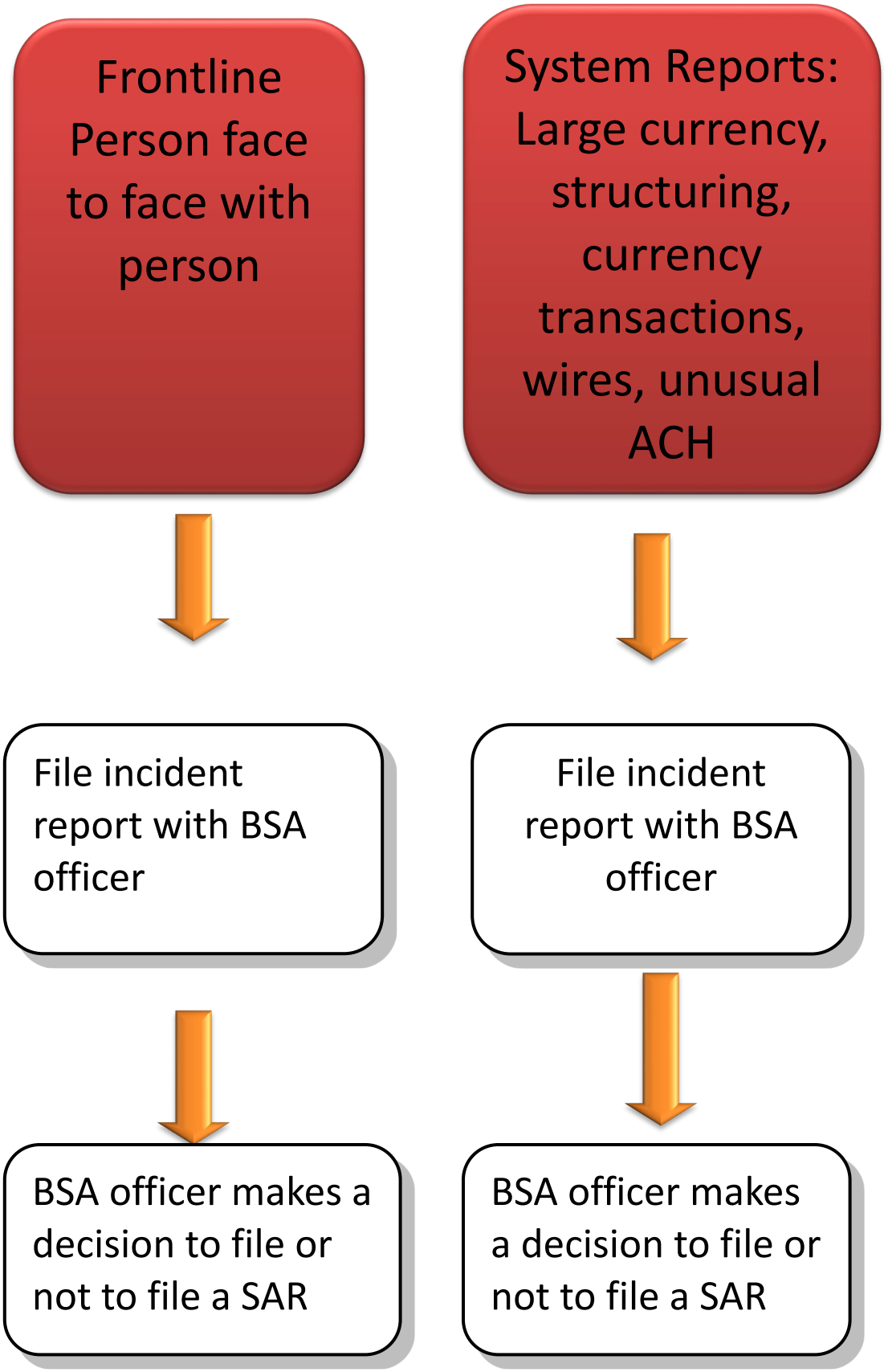
• An issuer of money orders or traveler's checks is not required to report a transaction or pattern of transactions when the transactions were identified through a review of clearance records or other similar records and the transaction amount or aggregated transaction amount involves funds or other assets of less than $5,000.

7. Additional Reporting: The Bank Secrecy Act requires financial institutions to file a Currency Transaction Report (CTR) in accordance with the Department of the Treasury's implementing regulations (31 CFR § 1010.310) whenever a currency transaction exceeds $10,000. If a currency transaction exceeds $10,000 and is otherwise reportable as suspicious activity, the institution must file both a CTR (reporting the currency transaction) and a BSA SAR (reporting the suspicious activity). If a currency transaction is $10,000 or less and is otherwise reportable as a suspicious activity, the institution should only file a BSA SAR. Appropriate records must be maintained in each case.

© gettechnical inc 2021

FRONTLINE AND SYSTEM RED FLAGS

© gettechnical inc 2021



© gettechnical inc 2021

Money Laundering and Terrorist Financing "Red Flags" (2007)

The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and examiners recognize possible money laundering and terrorist financing schemes. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity that May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A customer provides an individual tax identification number after having previously used a Social Security number.
- A customer uses different tax identification numbers with variations of his or her name.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer's home or business telephone is disconnected.
- The customer's background differs from that which would be expected on the basis of his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer is a trust, shell company, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner's identity.

Efforts to Avoid Reporting or Recordkeeping Requirement

© gettechnical inc 2021

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as non-cooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $10,000, to evade Currency Transaction Report (CTR) filing requirements.

Funds Transfers

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

Automated Clearing House Transactions

© gettechnical inc 2021

• Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.

• TPSPs have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.

• Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.

• Unusually high level of transactions initiated over the Internet or by telephone.

• National Automated Clearing House Association (NACHA) information requests indicate potential concerns with the bank's usage of the ACH system.

Computer Intrusion

Computer Intrusion is defined as "gaining access to a computer system of a financial institution to:

- Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
- Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
- Damage, disable or otherwise affect critical systems of the institution."

Activity Inconsistent with the Customer's Business

• The currency transaction patterns of a business show a sudden change inconsistent with normal activities.

• A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.

• A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.

• Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.

• The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.

• Goods or services purchased by the business do not match the customer's stated line of business.

• Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

Lending Activity

• Loans secured by pledged assets held by third parties unrelated to the borrower.

© gettechnical inc 2021

- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.
- Loans that lack a legitimate business purpose, provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

Changes in Bank-to-Bank Transactions

- The size and frequency of currency deposits increases rapidly with no corresponding increase in noncurrency deposits.
- A bank is unable to track the true accountholder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank's location.
- Changes in currency-shipment patterns between correspondent banks are significant.

Cross-Border Financial Institution Transactions[1]

- U.S. bank increases sales or exchanges of large denomination U.S. bank notes to Mexican financial institution(s).
- Large volumes of small denomination U.S. banknotes being sent from Mexican casas de cambio to their U.S. accounts via armored transport or sold directly to U.S. banks. These sales or exchanges may involve jurisdictions outside of Mexico.
- Casas de cambio direct the remittance of funds via multiple funds transfers to jurisdictions outside of Mexico that bear no apparent business relationship with the casas de cambio. Funds transfer recipients may include individuals, businesses, and other entities in free trade zones.
- Casas de cambio deposit numerous third-party items, including sequentially numbered monetary instruments, to their accounts at U.S. banks.
- Casas de cambio direct the remittance of funds transfers from their accounts at Mexican financial institutions to accounts at U.S. banks. These funds transfers follow the deposit of currency and third-party items by the casas de cambio into their Mexican financial institution.

[1] FinCEN Advisory FIN-2006-A003, Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States, April 28, 2006.

© gettechnical inc 2021

Trade Finance

- Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- Customers conducting business in high-risk jurisdictions.
- Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.
- Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties should prompt additional OFAC review.

Privately Owned Automated Teller Machines

- Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.
- Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armored car contracts, lending arrangements, or other appropriate documentation.

Insurance

- A customer purchases products with termination features without concern for the product's investment performance.

© gettechnical inc 2021

- A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
- A customer purchases product that appears outside the customer's normal range of financial wealth or estate planning needs.
- A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.
- A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.

Shell Company Activity

- A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).
- Payments to or from the company have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- Transacting businesses share the same address, provide only a registered agent's address, or have other address inconsistencies.
- Unusually large number and variety of beneficiaries are receiving funds transfers from one company.
- Frequent involvement of multiple jurisdictions or beneficiaries located in high-risk offshore financial centers.
- A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Purpose of the shell company is unknown or unclear.

Embassy and Foreign Consulate Accounts

© gettechnical inc 2021

- Official embassy business is conducted through personal accounts.
- Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.
- Accounts are funded through substantial currency transactions.
- Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

Employees

- Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.
- Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- Employee is reluctant to take a vacation.

Other Unusual or Suspicious Customer Activity

- Customer frequently exchanges small-dollar denominations for large-dollar denominations.
- Customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Customer purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold.
- Customer purchases a number of open-end stored value cards for large amounts. Purchases of stored value cards are not commensurate with normal business activities.
- Customer receives large and frequent deposits from on-line payments systems yet has no apparent on-line or auction business.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- Customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area, despite the availability of such services at an institution closer to them.
- Customer repeatedly uses a bank or branch location that is geographically distant from the customer's home or office without sufficient business purpose.

© gettechnical inc 2021

- Customer exhibits unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, several individuals arrive together, enter frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.
- Unusual use of trust funds in business transactions or other financial activity.
- Customer uses a personal account for business purposes.
- Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.
- Customer makes multiple and frequent currency deposits to various accounts that are purportedly unrelated.
- Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.
- Customer makes high-value transactions not commensurate with the customer's known incomes.

Potentially Suspicious Activity that May Indicate Terrorist Financing

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance "Guidance for Financial Institutions in Detecting Terrorist Financing" provided by the FATF.[2] FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

Activity Inconsistent with the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).

[2] Guidance for Financial Institutions in Detecting Terrorist Financing, April 24, 2002, is available at www.fatf-gafi.org.

© gettechnical inc 2021

- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to high-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in high-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from high-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from high-risk locations open accounts.
- Funds are sent or received via international transfers from or to high-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

Structuring

Structuring transactions to evade BSA reporting and certain recordkeeping requirements can result in civil and criminal penalties under the BSA. Under the BSA (31 USC 5324), no person shall, for the purpose of evading the Currency Transaction Report (CTR) or a geographic targeting order

© gettechnical inc 2021

reporting requirement, or certain BSA recordkeeping requirements:

- Cause or attempt to cause a bank to fail to file a CTR or a report required under a geographic targeting order or to maintain a record required under BSA regulations.
- Cause or attempt to cause a bank to file a CTR or report required under a geographic targeting order, or to maintain a BSA record that contain a material omission or misstatement of fact.
- Structure, as defined above, or attempt to structure or assist in structuring, any transaction with one or more banks.

The definition of structuring, as set forth in 31 CFR 1010.100 (which was implemented before a Patriot Act provision extended the prohibition on structuring to geographic targeting orders and BSA recordkeeping requirements) states, "a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [CTR filing requirements]." "In any manner" includes, but is not limited to, breaking down a single currency sum exceeding $10,000 into smaller amounts that may be conducted as a series of transactions at or less than $10,000. The transactions need not exceed the $10,000 CTR filing threshold at any one bank on any single day in order to constitute structuring.

Money launderers and criminals have developed many ways to structure large amounts of currency to evade the CTR filing requirements. Unless currency is smuggled out of the United States or commingled with the deposits of an otherwise legitimate business, any money laundering scheme that begins with a need to convert the currency proceeds of criminal activity into more legitimate-looking forms of financial instruments, accounts, or investments, will likely involve some form of structuring. Structuring remains one of the most commonly reported suspected crimes on Suspicious Activity Reports (SARs).

Bank employees should be aware of and alert to structuring schemes. For example, a customer may structure currency deposit or withdrawal transactions, so that each is less than the $10,000 CTR filing threshold; use currency to purchase official bank checks, money orders, or traveler's checks with currency in amounts less than $10,000 (and possibly in amounts less than the $3,000 recordkeeping threshold for the currency purchase of monetary instruments to avoid having to produce identification in the process); or exchange small bank notes for large ones in amounts less than $10,000.
However, two transactions slightly under the $10,000 threshold conducted days or weeks apart may not necessarily be structuring. For example, if a customer deposits $9,900 in currency on Monday and deposits $9,900 in currency on Wednesday, it should not be assumed that structuring has occurred. Instead, further review and research may be necessary to determine the nature of the transactions, prior account history, and other relevant customer information to assess whether the activity is suspicious. Even if structuring has not occurred, the bank should review the transactions for suspicious activity.

In addition, structuring may occur before a customer brings the funds to a bank. In these instances, a bank may be able to identify the aftermath of structuring. Deposits of monetary instruments that may have been purchased elsewhere might be structured to evade the CTR filing requirements or the recordkeeping requirements for the currency purchase of monetary

© gettechnical inc 2021

instruments. These instruments are often numbered sequentially in groups totaling less than $10,000 or $3,000; bear the same handwriting (for the most part) and often the same small mark, stamp, or initials; or appear to have been purchased at numerous places on the same or different days.

© gettechnical inc 2021

BSA INCIDENT REPORT (2018 CHANGES)

To: BSA Officer

From:

Step One: Accountholder's Name:

Account No

Step Two: Check the boxes that apply and type any use information regarding the "other" transactions or incident.

Structuring

- ☐ Alters transaction to avoid BSA recordkeeping requirement
- ☐ Alters transaction to avoid CTR requirement
- ☐ Customer cancels transaction to avoid BSA reporting and recordkeeping requirements
- ☐ Multiple transactions below BSA recordkeeping threshold
- ☐ Multiple transactions below CTR threshold
- ☐ Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements
- ☐ Other

Terrorist Financing

- ☐ Known or suspected terrorist / terrorist organization
- ☐ Other

Fraud

- ☐ ACH
- ☐ Business loan
- ☐ Check
- ☐ Consumer loan
- ☐ Credit/Debit card
- ☐ Mass-marketing
- ☐ Pyramid scheme
- ☐ Wire

Money laundering

- ☐ Exchanges small bills for large bills or vice versa
- ☐ Funnel Account
- ☐ Suspicion concerning the physical condition of funds
- ☐ Suspicion concerning the source of funds
- ☐ Suspicious designation of beneficiaries, assignees or joint owners
- ☐ Suspicious EFT/Wire transfers
- ☐ Suspicious exchange of currencies
- ☐ Suspicious receipt of government payments/benefits
- ☐ Suspicious use of multiple accounts
- ☐ Suspicious use of noncash monetary instruments
- ☐ Suspicious use of third-party transactors (straw-man)
- ☐ Trade Based Money Laundering / Black Market Peso Exchange
- ☐ Transaction out of pattern for customer(s)
- ☐ Other

Identification / Documentation

- ☐ Changes spelling or arrangement of name
- ☐ Multiple individuals with same or similar identities
- ☐ Provided questionable or false documentation
- ☐ Refused or avoided request for documentation
- ☐ Single individual with multiple identities
- ☐ Other

Other suspicious activities

- ☐ Account takeover
- ☐ Bribery or gratuity
- ☐ Counterfeit instruments
- ☐ Elder financial exploitation
- ☐ Embezzlement/theft/disappearance of funds
- ☐ Forgeries
- ☐ Human smuggling

© gettechnical inc

- ☐ Human trafficking
- ☐ Identity theft
- ☐ Little or no concern for product performance penalties, fees, or tax consequences
- ☐ Misuse of "free look"/cooling off/right of rescission
- ☐ Misuse of position or self-dealing
- ☐ Suspected public/private corruption (domestic)
- ☐ Suspected public/private corruption (foreign)
- ☐ Suspicious use of informal value transfer system
- ☐ Suspicious use of multiple transaction locations
- ☐ Transaction with no apparent economic, business, or lawful purpose
- ☐ Two or more individuals working together
- ☐ Unauthorized electronic intrusion
- ☐ Unlicensed or unregistered MSB
- ☐ Other

Mortgage fraud

- ☐ Application fraud
- ☐ Appraisal fraud
- ☐ Foreclosure fraud
- ☐ Loan modification fraud
- ☐ Reverse mortgage fraud
- ☐ Other

Was any of the following product type(s) involved in the suspicious activity? Check all that apply:

- ☐ Bonds/Notes
- ☐ Commercial mortgage
- ☐ Commercial paper
- ☐ Credit card
- ☐ Debit card
- ☐ Home equity loan
- ☐ Home equity line of credit
- ☐ Prepaid access
- ☐ Residential mortgage
- ☐ Other

Were any of the following instrument type(s)/payment mechanism(s) involved in the suspicious activity? Check all that apply:

- ☐ Bank/cashier's check
- ☐ Foreign currency
- ☐ Funds transfer
- ☐ Deposit account
- ☐ Microcap Security
- ☐ Gaming instruments
- ☐ Government payment
- ☐ Money orders
- ☐ Personal/Business check
- ☐ Travelers checks
- ☐ U.S. Currency
- ☐ Other:

Cyber Crimes

- ☐ Against Financial Institution
- ☐ Against Customer

Step 3: Written Explanation or Other commentary:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

TRACK TWO: SYSTEMS

Suspicious Activity Reporting — Overview (2014)

Objective. *Assess the bank's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.*

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Within this system, FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. Examiners should focus on evaluating a bank's policies, procedures, and processes to identify, evaluate, and report suspicious activity. However, as part of the examination process, examiners should review individual SAR filing decisions to determine the effectiveness of the bank's suspicious activity identification, evaluation, and reporting process. Banks, bank holding companies, and their subsidiaries are required by federal regulations[53] to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing).[54]
  - Is designed to evade the BSA or its implementing regulations.[55]
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit,

[53] Refer to 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System) (Federal Reserve); 12 CFR 353 (Federal Deposit Insurance Corporation)(FDIC); 12 CFR 748 (National Credit Union Administration)(NCUA); 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency)(OCC); and 31 CFR 1020.320 (FinCEN).

[54] FinCEN issued guidance identifying certain BSA expectations for banks offering services to marijuana-related businesses, including expectations for filing SARs, FIN-2014-G001, February 14, 2014.

[55] Refer to Appendix G ("Structuring") for additional guidance.

© gettechnical inc

or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

Safe Harbor for Banks From Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides that a bank and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.[56]

Systems to Identify, Research, and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that the bank has an adequate and effective BSA compliance program. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. The bank should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the bank's overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

Generally, effective suspicious activity monitoring and reporting systems include five key components (refer to Appendix S "Key Suspicious Activity Monitoring Components"). The components, listed below, are interdependent, and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance. The five key components to an effective monitoring and reporting system are:

[56] The agencies incorporated the statutory expansion of the safe harbor by cross-referencing section 5318(g) in their SAR regulations. The OCC and FinCEN amended their SAR regulations to make clear that the safe harbor also applies to a disclosure by a bank made jointly with another financial institution for purposes of filing a joint SAR (see 12 CFR 21.11(l) and 31 CFR 1020.320(e)), respectively.

- Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
- Managing alerts.
- SAR decision making.
- SAR completion and filing.
- Monitoring and SAR filing on continuing activity.

These components are present in banks of all sizes. However, the structure and formality of the components may vary. Larger banks typically have greater differentiation and distinction between functions, and may devote entire departments to the completion of each component. Smaller banks may use one or more employees to complete several tasks (e.g., review of monitoring reports, research activity, and completion of the actual SAR). Policies, procedures, and processes should describe the steps the bank takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, SAR completion and filing, and monitoring and SAR filing on continuing activity.

Identification of Unusual Activity

Banks use a number of methods to identify potentially suspicious activity, including but not limited to activity identified by employees during day-to-day operations, law enforcement inquiries, or requests, such as those typically seen in section 314(a) and section 314(b) requests, advisories issued by regulatory or law enforcement agencies, transaction and surveillance monitoring system output, or any combination of these.

Employee Identification

During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity. Banks should implement appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring system includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research.

Law Enforcement Inquiries and Requests

Banks should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSL), and section 314(a) requests.[57]

[57] Refer to core overview section, "Information Sharing," page 92, for a discussion on section 314(a) requests.

Mere receipt of any law enforcement inquiry does not, by itself, require the filing of a SAR by the bank. Nonetheless, a law enforcement inquiry may be relevant to a bank's overall risk assessment of its customers and accounts. For example, the receipt of a grand jury subpoena should cause a bank to review account activity for the relevant customer.[58] A bank should assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program.

The bank should determine whether a SAR should be filed based on all customer information available. Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the bank.

National Security Letters

NSLs are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and Internet service providers.[59]
- Information from credit bureaus.[60]
- Financial records from financial institutions.[61]

NSLs are highly confidential documents; for that reason, examiners do not review or sample specific NSLs.[62] Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a bank files a SAR after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the bank.

Questions regarding NSLs should be directed to the bank's local FBI field office. Contact information for the [F B I] field offices can be found at www.fbi.gov.

---

[58] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, May 2006, pages 42 – 44, on the FinCEN Web site.

[59] Electronic Communications Privacy Act, 18 USC 2709.

[60] Fair Credit Reporting Act, 15 USC 1681u.

[61] Right to Financial Privacy Act of 1978, 12 USC 3401 *et seq.*

[62] Refer to the Bank Secrecy Act Advisory Group, *The SAR Activity Review — Trends, Tips & Issues*, Issue 8, April 2005 for further information on NSLs which is available on the FinCEN Web site.

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system, sometimes referred to as a manual transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographies) and includes a manual review of various reports generated by the bank's MIS or vendor systems in order to identify unusual activity. Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, ATM transaction reports, and nonsufficient funds (NSF) reports. Many MIS or vendor systems include filtering models for identification of potentially unusual activity. The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its higher-risk products, services, customers, entities, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Thresholds selected by management for the production of transaction reports should enable management to detect unusual activity. Upon identification of unusual activity, assigned personnel should review CDD and other pertinent information to determine whether the activity is suspicious. Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each bank should evaluate and identify filtering criteria most appropriate for their bank. The programming of the bank's monitoring systems should be independently reviewed for reasonable filtering criteria. Typical transaction monitoring reports are as follows.

Currency activity reports. Most vendors offer reports that identify all currency activity or currency activity greater than $10,000. These reports assist bankers with filing CTRs and identifying suspicious currency activity. Most bank information service providers offer currency activity reports that can filter transactions using various parameters, for example:

- Currency activity including multiple transactions greater than $10,000.
- Currency activity (single and multiple transactions) below the $10,000 reporting requirement (e.g., between $7,000 and $10,000).
- Currency transactions involving multiple lower dollar transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., $30,000).
- Currency transactions aggregated by customer name, taxpayer identification number, or customer information file number.

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, significantly enhance a bank's ability to identify and evaluate unusual currency transactions.

Funds transfer records. The BSA requires banks to maintain records of funds transfer in amounts of $3,000 and above. Periodic review of this information can assist banks in identifying patterns of unusual activity. A periodic review of the funds transfer records in banks with low funds transfer activity is usually sufficient to identify unusual activity. For

banks with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses. Each bank should establish its own filtering criteria for both individuals and businesses. Noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, banks may need to conduct a global relationship review to determine if a SAR is warranted.

Monetary instrument records. Records for monetary instrument sales are required by the BSA. Such records can assist the bank in identifying possible currency structuring through the purchase of cashier's checks, official bank checks, money orders, or traveler's checks in amounts of $3,000 to $10,000. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees. Reviews for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system, sometimes referred to as an automated account monitoring system, can cover multiple types of transactions and use various rules to identify potentially suspicious activity. In addition, many can adapt over time based on historical activity, trends, or internal peer comparison. These systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the bank's core data processing system. Banks that are large, operate in many locations, or have a large volume of higher-risk customers typically use surveillance monitoring systems.

Surveillance monitoring systems include rule-based and intelligent systems. Rule-based systems detect unusual transactions that are outside of system-developed or management-established "rules." Such systems can consist of few or many rules, depending on the complexity of the in-house or vendor product. These rules are applied using a series of transaction filters or a rules engine. Rule-based systems are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than $10,000). Rule-based systems can apply multiple rules, overlapping rules, and filters that are more complex. For example, rule-based systems can initially apply a rule, or set of criteria to all accounts within a bank (e.g., all retail customers), and then apply a more refined set of criteria to a subset of accounts or risk category of accounts (e.g., all retail customers with direct deposits). Rule-based systems can also filter against individual customer-account profiles.

Intelligent systems are adaptive and can filter transactions, based on historical account activity or compare customer activity against a pre-established peer group or other relevant data. Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

Relative to surveillance monitoring, system capabilities and thresholds refer to the parameters or filters used by banks in their monitoring processes. Parameters and filters should be reasonable and tailored to the activity that the bank is trying to identify or control. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed. For example, a bank may discover that its filter for cash structuring is triggered only by a daily cash transaction in excess of $10,000. The bank may need to refine this filter in order to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions that are slightly under the CTR threshold.

Once established, the bank should review and test system capabilities and thresholds on a periodic basis. This review should focus on specific parameters or filters in order to ensure that intended information is accurately captured and that the parameter or filter is appropriate for the bank's particular risk profile.

Understanding the filtering criteria of a surveillance monitoring system is critical to assessing the effectiveness of the system. System filtering criteria should be developed through a review of specific higher-risk products and services, customers and entities, and geographies. System filtering criteria, including specific profiles and rules, should be based on what is reasonable and expected for each type of account. Monitoring accounts purely based on historical activity can be misleading if the activity is not actually consistent with similar types of accounts. For example, an account may have a historical transaction activity that is substantially different from what would normally be expected from that type of account (e.g., a check-cashing business that deposits large sums of currency versus withdrawing currency to fund the cashing of checks).

The authority to establish or change expected activity profiles should be clearly defined through policies and procedures. Controls should ensure limited access to the monitoring systems, and changes should generally require the approval of the BSA compliance officer or senior management.

Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks. Management should also periodically review and test the filtering criteria and thresholds established to ensure that they are still effective. In addition, the monitoring system's programming methodology and effectiveness should be independently validated to ensure that the models are detecting potentially suspicious activity. The independent validation should also verify the policies in place and that management is complying with those policies.

Managing Alerts

Alert management focuses on processes used to investigate and evaluate identified unusual activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification. Banks should have policies, procedures, and processes in place for referring unusual activity from all areas of the bank or business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The bank should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the bank's overall risk profile and the volume of transactions. Additionally, a bank should ensure that the assigned staff possess the requisite experience levels and are provided with comprehensive and ongoing training to maintain their expertise. Staff should also be provided with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

Internal research tools include, but are not limited to, access to account systems and account information, including CDD and EDD information. CDD and EDD information assist banks in evaluating if the unusual activity is considered suspicious. For additional information, refer to the core overview section, "Customer Due Diligence," page 56. External research tools may include widely available Internet media search tools, as well those accessible by subscription. After thorough research and analysis, investigators should document conclusions including any recommendation regarding whether or not to file a SAR.

When multiple departments are responsible for researching unusual activities (i.e., the BSA department researches BSA-related activity and the Fraud department researches fraud-related activity), the lines of communication between the departments must remain open. This allows banks with bifurcated processes to gain efficiencies by sharing information, reducing redundancies, and ensuring all suspicious activity is identified, evaluated, and reported.

If applicable, reviewing and understanding suspicious activity monitoring across the organizations' affiliates, subsidiaries, and business lines may enhance a banking organization's ability to detect suspicious activity, and thus minimize the potential for financial losses, increased legal or compliance expenses, and reputational risk to the organization. Refer to the expanded overview section, "BSA/AML Compliance Program Structures," page 155, for further guidance.

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[63] and certain other crimes above prescribed dollar thresholds.

[63] If a bank knows, suspects, or has reason to suspect that a customer may be linked to terrorist activity against the United States, the bank should immediately call FinCEN's Financial Institutions terrorist hot line toll-free number (866) 556-3974. Similarly, if any other suspected violation — such as an ongoing money laundering

However, banks are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement. When evaluating suspicious activity and completing the SAR, banks should, to the best of their ability, identify the characteristics of the suspicious activity. Suspicious Activity Information, Part II of the SAR provides a number of categories with different types of suspicious activity. Within each category, there is the option of selecting "Other" if none of the suspicious activities apply. However, the use of "Other" should be limited to situations that cannot be broadly identified within the categories provided.

SAR Decision Making

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). The bank should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. When the bank uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions. Banks should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision is based on unique facts and circumstances, no single form of documentation is required when a bank decides not to file.[64]

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[65]

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is

scheme — requires immediate attention, the bank should notify the appropriate federal banking and law enforcement agencies. In either case, the bank must also file a SAR.

[64] Bank Secrecy Act Advisory Group, "Section 4 — Tips on SAR Form Preparation & Filing," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 38, on the FinCEN Web site.

[65] Refer to Appendix R ("Interagency Enforcement Statement") for additional information.

accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the federal banking agencies. FinCEN's guidelines have suggested that banks should report continuing suspicious activity by filing a report at least every 90 calendar days. Subsequent guidance permits banks with SAR requirements to file SARs for continuing activity after a 90 day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing. Banks may also file SARs on continuing activity earlier than the 120-day deadline if the bank believes the activity warrants earlier review by law enforcement.[66] This practice notifies law enforcement of the continuing nature of the activity in aggregate. In addition, this practice reminds the bank that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as bank management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

Banks should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that a bank maintain a particular account, the bank should ask for a written request. The written request should indicate that the agency has requested that the bank maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by a bank in accordance with its own standards and guidelines.[67]

The bank should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts. The procedures should include:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
- Criteria for when analysis of the overall customer relationship is necessary.
- Criteria for whether and, if so, when to close the account.
- Criteria for when to notify law enforcement, if appropriate.

SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SARs are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. FinCEN developed a new electronic BSA Suspicious Activity Report (BSAR) that replaced FinCEN SAR-DI form TD F 90-22.47. The BSAR provides a uniform data collection format that can be used across multiple industries. As of April 1, 2013, the BSAR is mandatory and must be filed through

[66] Refer to Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report, Question #16.

[67] Refer to *Requests by Law Enforcement for Financial Institutions to Maintain Accounts*, June 13, 2007.

FinCEN's BSA E-Filing System. The BSAR does not create or otherwise change existing statutory and regulatory expectations for banks.

The BSAR includes a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. Certain fields in the BSAR are marked as "critical" for technical filing purposes. This means the BSA E-Filing System does not accept filings in which these fields are left blank. For these items, the bank must either provide the requested information or check the "unknown" box that is provided with each critical field. Banks should provide the most complete filing information available consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.[68]

Banks should report the information that they know, or that otherwise arises, as part of their case reviews. Other than the critical fields, the addition of the new and expanded data elements does not create an expectation that banks will revise internal programs, or develop new programs, to capture information that reflects the expanded lists.[69] Refer to Appendix T for additional information on filing through the BSA E-Filing System.

Timing of a SAR Filing

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.[70]

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The bank's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a

[68] Refer to *Filing FinCEN's new Currency Transaction Report and Suspicious Activity Report*, FIN-2012-G002, March 29, 2012.

[69] *Id.*

[70] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 1, October 2000, page 27.

determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation.[71]

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. What constitutes a "reasonable period of time" varies according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that a bank has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.[72]

For situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the bank's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.[73]

SAR Quality

Banks are required to file SARs that are complete, thorough, and timely. Banks should include all known subject information on the SAR. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the section, as stated on the SAR, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

To inform and assist banks in reporting instances of suspected money laundering, terrorist financing, and fraud, FinCEN issues advisories and guidance containing examples of "red flags." In order to assist law enforcement in its efforts to target these activities, FinCEN requests that banks check the appropriate box(es) in the Suspicious Activity Information

[71] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 44. For examples of when the date of initial detection occurs, refer to *SAR Activity Review — Trends, Tips, and Issues*, Issue 14, October 2008, page 38.

[72] *Id*.

[73] For suspicious activity related to terrorist activity, institutions may also call FinCEN's Financial Institution's terrorist hot line's toll-free number (866) 556-3974 (seven days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

section and include certain key terms in the narrative section of the SAR. The advisories and guidance can be found on FinCEN Web site.[74]

By their nature, SAR narratives are subjective, and examiners generally should not criticize the bank's interpretation of the facts. Nevertheless, banks should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included within the SAR. The BSAR accepts a single, Microsoft Excel-compatible comma separated value (csv) file no larger than one (1) megabyte as an attachment as part of the report. This capability allows a bank to include transactional data such as specific financial transactions and funds transfers or other analytics that are more readable or usable in this format than it would be if otherwise included in the narrative. Such an attachment is be considered a part of the narrative and is not considered to be a substitute for the narrative. For example, narratives should not simply state "see attachment" if the bank included a csv attachment. As with other information that may be prepared in connection with the filing of a SAR, an attachment is considered supporting documentation and should be treated as confidential to the extent that it indicates the existence of a SAR.

More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist banks in writing, and assist examiners in evaluating, SAR narratives.[75]

Notifying Board of Directors of SAR Filings

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties, while being mindful of the confidential nature of the SAR.[76]

[74] For more information, refer to SAR Advisory Key Terms on the FinCEN Web site.

[75] Guidance to assist banks in filing SARs can be found in the *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements* Release Date October 2012, Version 1.2. Other guidance available from FinCEN includes "*Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting*" (October 10, 2007).

[76] As noted in the Bank Secrecy Act Advisory Group's *The SAR Activity Review — Trends, Tips & Issues*, Issue 2, June 2001, "In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised."

Record Retention and Supporting Documentation

Banks must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. The bank can retain copies in paper or electronic format. Additionally, banks must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all documents or records that assisted a bank in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or federal banking agency.[77]

Prohibition of SAR Disclosure

No bank, and no director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR. [78] Furthermore, FinCEN and the federal banking agencies take the position that a bank's internal controls for the filing of SARs should minimize the risks of disclosure.

A bank or its agent may reveal the existence of a SAR to fulfill responsibilities consistent with the BSA, provided no person involved in a suspicious transaction is notified that the transaction has been reported. The underlying facts, transactions, and supporting documents of a SAR may be disclosed to another financial institution for the preparation of a joint SAR, or in connection with certain employment references or termination notices to the full extent authorized in 31 USC 5318(g)(2)(B). The sharing of a SAR by a bank or its agent with certain permissible entities within the bank's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act is also allowed.

Any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement[79] or federal banking agency, shall decline to produce the SAR or to provide

[77] Refer to *Suspicious Activity Report Supporting Documentation*, June 13, 2007.

[78] FinCEN and the OCC issued final rules amending the confidentiality provisions of suspicious activity reports. The rules clarify how, when, and to whom SAR information, and the existence of a SAR may be disclosed. Refer to 75 Fed. Reg. 75576 (December 3, 2010) (OCC) and 75 Fed. Reg. R 75593 (December 3, 2010) (FinCEN).

[79] Examples of agencies to which a SAR or the information contained therein could be provided include: the criminal investigative services of the armed forces; the Bureau of Alcohol, Tobacco, and Firearms; an attorney general, district attorney, or state's attorney at the state or local level; the Drug Enforcement Administration; the Federal Bureau of Investigation; the Internal Revenue Service or tax enforcement agencies at the state level; the Office of Foreign Assets Control; a state or local police department; a United States Attorney's Office; Immigration and Customs Enforcement; the U.S. Postal Inspection Service; and the U.S. Secret Service. For additional information, refer to Bank Secrecy Act Advisory Group, "Section 5—Issues and Guidance," *The SAR Activity Review—Trends, Tips & Issues,* Issue 9, October 2005, page 44 on the FinCEN Web site.

any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(A)(i). FinCEN and the bank's federal banking agency should be notified of any such request and of the bank's response.

Examiners should follow their respective agency's protocol on discovery of the improper disclosure of a SAR. Examiners also should ensure the bank has notified the appropriate federal banking agency and FinCEN of the improper disclosure.

Sharing SARs With Head Offices, Controlling Companies, and Certain U.S. Affiliates

Previously issued guidance clarified that sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a bank's compliance with applicable laws and regulations. [80]

A controlling company as defined in the guidance includes:

- A bank holding company (BHC), as defined in section 2 of the BHC Act.
- A savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act.
- A company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an industrial loan company or parent company.

The guidance confirms that:

- A U.S. branch or agency of a foreign bank may share a SAR with its head office outside the United States.
- A U.S. bank may share a SAR with controlling companies whether domestic or foreign.

In addition, a bank that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate provided the affiliate is subject to a SAR regulation.[81] An affiliate is defined as any company under common control with, or controlled by, that depository institution. Under "common control'' means that another company:

- Directly or indirectly or acting through one or more other persons owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution; or

[80] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies*, issued by FinCEN, Federal Reserve, FDIC, OCC, and OTS, January 20, 2006.

[81] *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates,* issued by FinCEN, FIN-2010-G006, November 23, 2010.

- Controls in any manner the election of a majority of the directors or trustees of the company and the depository institution.

Controlled by means that the depository institution:

- Directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or

- Controls in any manner the election of a majority of the directors or trustees of the company. See 12 USC 1841(a)(2).

Because foreign branches of U.S. banks are regarded as foreign banks for the purposes of the BSA, they are affiliates that are not subject to a SAR regulation. Accordingly, a U.S. bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches.

Banks should maintain appropriate arrangements with head offices, controlling companies, and affiliates to protect the confidentiality of SARs. The bank should have policies and procedures in place to protect the confidentiality of the SAR as part of their internal controls.

Examination Procedures

Suspicious Activity Reporting

Objective. *Assess the bank's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.*

Initially, examiners may elect to "map out" the process the bank follows to monitor for, identify, research, and report suspicious activities. Once the examiner has an understanding of the process, the examiner should follow an alert through the entire process.

Identification of Unusual Activity

1. Review the bank's policies, procedures, and processes for identifying, researching, and reporting suspicious activity. Determine whether they include the following:
   - Lines of communication for the referral of unusual activity to appropriate personnel.
   - Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities.
   - Monitoring systems used to identify unusual activity.
   - Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests (e.g., grand jury subpoenas, section 314(a) requests, or National Security Letters (NSL)) for suspicious activity. NSLs are highly confidential documents; as such, examiners do not review or sample specific NSLs. Instead, examiners should evaluate the policies, procedures, and processes for:
     - Responding to NSLs.
     - Evaluating the account of the target for suspicious activity.
     - Filing SARs, if necessary.
     - Handling account closures.
2. Review the bank's monitoring systems and how the system(s) fits into the bank's overall suspicious activity monitoring and reporting process. Complete the appropriate examination procedures that follow. When evaluating the effectiveness of the bank's monitoring systems, examiners should consider the bank's overall risk profile (higher-risk products, services, customers, entities, and geographic locations), volume of transactions, and adequacy of staffing.

Transaction (Manual Transaction) Monitoring

3. Review the bank's transaction monitoring reports. Determine whether the reports capture all areas that pose money laundering and terrorist financing risks. Examples of these reports include: currency activity reports, funds transfer reports, monetary instrument sales reports, ATM transaction reports, large item reports, significant balance change reports, nonsufficient funds (NSF) reports, and nonresident alien (NRA) reports.

4. Determine whether the bank's transaction monitoring systems use reasonable filtering criteria whose programming has been independently verified. Determine whether the monitoring systems generate accurate reports at a reasonable frequency.

Surveillance (Automated Account) Monitoring

5. Identify the types of customers, products, and services that are included within the surveillance monitoring system.

6. Identify the system's methodology for establishing and applying expected activity or profile filtering criteria and for generating monitoring reports. Determine whether the system's filtering criteria are reasonable.

7. Determine whether the programming of the methodology has been independently validated.

8. Determine that controls ensure limited access to the monitoring system and sufficient oversight of assumption changes.

Managing Alerts

9. Determine whether the bank has policies, procedures, and processes to ensure the timely generation of, review of, and response to reports used to identify unusual activities.

10. Determine whether policies, procedures, and processes require appropriate research when monitoring reports identify unusual activity.

11. Evaluate the bank's policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. The process should ensure that all applicable information (e.g., criminal subpoenas, NSLs, and section 314(a) requests) is effectively evaluated.

12. Verify that staffing levels are sufficient to review reports and alerts and investigate items, and that staff possess the requisite experience level and proper investigatory tools. The volume of system alerts and investigations should not be tailored solely to meet existing staffing levels.

13. Determine whether the bank's SAR decision process appropriately considers all available CDD and EDD information.

SAR Decision Making

14. Determine whether the bank's policies, procedures, and processes include procedures for:

    - Documenting decisions not to file a SAR.
    - Escalating issues identified as the result of repeat SAR filings on accounts.
    - Considering closing accounts as a result of continuous suspicious activity.

SAR Completion and Filing

15. Determine whether the bank's policies, procedures, and processes provide for:

    - Completing, filing, and retaining SARs and their supporting documentation.
    - Reporting SARs to the board of directors, or a committee thereof, and informing senior management.
    - Sharing SARs with head offices and controlling companies, as necessary.

Transaction Testing

Transaction testing of suspicious activity monitoring systems and reporting processes is intended to determine whether the bank's policies, procedures, and processes are adequate and effectively implemented. Examiners should document the factors they used to select samples and should maintain a list of the accounts sampled. The size and the sample should be based on the following:

- Weaknesses in the account monitoring systems.
- The bank's overall BSA/AML risk profile (e.g., number and type of higher-risk products, services, customers, entities, and geographies).
- Quality and extent of review by audit or independent parties.
- Prior examination findings.
- Recent mergers, acquisitions, or other significant organizational changes.
- Conclusions or questions from the review of the bank's SARs.

Refer to Appendix O ("Examiner Tools for Transaction Testing") for additional guidance.

16. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, sample specific customer accounts to review the following:

    - Suspicious activity monitoring reports.
    - CTR download information.
    - Higher-risk banking operations (products, services, customers, entities, and geographies).
    - Customer activity.
    - Subpoenas received by the bank.
    - Decisions not to file a SAR.

17. For the customers selected previously, obtain the following information, if applicable:

    - CIP and account-opening documentation.
    - CDD documentation.

- Two to three months of account statements covering the total customer relationship and showing all transactions.
- Sample items posted against the account (e.g., copies of checks deposited and written, debit or credit tickets, and funds transfer beneficiaries and originators).
- Other relevant information, such as loan files and correspondence.

18. Review the selected accounts for unusual activity. If the examiner identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e., the sort of activity in which the customer is normally expected to engage). When reviewing for unusual activity, consider the following:
    - For individual customers, whether the activity is consistent with CDD information (e.g., occupation, expected account activity, and sources of funds and wealth).
    - For business customers, whether the activity is consistent with CDD information (e.g., type of business, size, location, and target market).
19. Determine whether the transaction or surveillance suspicious activity monitoring system detected the activity that the examiner identified as unusual.
20. For transactions identified as unusual, discuss the transactions with management. Determine whether the account officer demonstrates knowledge of the customer and the unusual transactions. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions.
21. Determine whether the bank has failed to identify any reportable suspicious activity.
22. From the results of the sample, determine whether the transaction or surveillance suspicious activity monitoring system effectively detects unusual or suspicious activity. Identify the underlying cause of any deficiencies in the monitoring systems (e.g., inappropriate filters, insufficient risk assessment, or inadequate decision making).
23. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of management's research decisions to determine the following:
    - Whether management decisions to file or not file a SAR are supported and reasonable.
    - Whether documentation is adequate.
    - Whether the decision process is completed and SARs are filed in a timely manner.
24. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, sample the SARs downloaded from the BSA-reporting database or the bank's internal SAR records. Review the quality of SAR content to assess the following:
    - SARs contain accurate information.

© gettechnical inc 2019

- SAR narratives are complete and thorough, and clearly explain why the activity is suspicious (i.e., the SAR narrative should not simply state “see attachment” if the bank included a csv file).

25. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity.

© gettechnical inc 2019

THE INVESTIGATION

© gettechnical inc 2021

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[3] and certain other crimes above prescribed dollar thresholds. However, banks are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement.

SAR Completion

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statutes	Explanation/Description
a	Bank Secrecy Act/Structuring/ Money Laundering	31 U.S.C. Section 5311 and 31 C.F.R. Chapter X Bank Secrecy Act 31 U.S.C. Section 5324 - Structuring Transactions to Evade Reporting 18 U.S.C. Section 1956 - Laundering of Monetary 18 U.S.C. Section 1957 - Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity	I. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction recordkeeping and reporting requirement under federal law and reporting requirement under federal law ii. The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or iii. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts including the background and possible purpose of the transaction. There are four types of structuring activities that are reportable: 1. To avoid generating any Currency Transaction Report, Form 8300 and supporting records, and to avoid any recordkeeping connected to monetary instruments. 2. To avoid the identification requirements, e.g. connected with non-bank money transmissions and purchase of monetary instruments. 3. To avoid suspicious detection and conventional monitoring thresholds and filters. 4. To avoid enhanced scrutiny or additional review frequently triggered by higher transaction amounts and thresholds. Note: 18 USC 1956 creates 3 basic categories of Money Laundering:

[3] If a bank knows, suspects, or has reason to suspect that a customer may be linked to terrorist activity against the United States, the bank should immediately call FinCEN's Financial Institutions Terrorist Hotline at the toll-free number: 866-556-3974. Similarly, if any other suspected violation — such as an ongoing money laundering scheme — requires immediate attention, the bank should notify the appropriate federal banking and law enforcement agencies. In either case, the bank must also file a SAR.

© gettechnical inc 2021

			1. Conducting/attempting to conduct one or more financial transactions with proceeds from Instruments specified unlawful activity; 2. Transporting/transmitting/transferring one or more monetary instruments or funds into or out of the United States with intent to promote carrying out of unlawful activity, to conceal or disguise the proceeds of specified unlawful activity, or to avoid a state or federal transaction reporting requirement; 3. Where property has been represented to be from specified unlawful activity (to cover law enforcement-related sting operations where the property is really clean.)

© gettechnical inc 2021

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statutes	Explanation/Description
b	Bribery / Gratuity	- Bank Bribery 18 U.S.C. Section 215	Anyone who, in connection with bank business, corruptly gives, offers or promises anything of value to a bank official with the intent to influence or reward that official
c	Check Fraud	18 U.S.C. Section 1344- Bank Fraud	This type of fraud takes on many forms including: altered checks; check kiting; charge-back check fraud; closed account fraud; and variations on check forgeries. Other common check fraud violations noted are the withdrawal of funds against checks with forged endorsements or maker's signatures and counterfeit checks.
d	Check Kiting	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657- Embezzlement, Theft or Misapplication of Funds	A practice in which an individual with accounts at two or more financial institutions intentionally utilizes the delay in the check clearing process to write checks from one account to deposit into the second account, all the while knowing that the first account does not have collected funds. The subject continues this cycle, moving checks between accounts, to make it appear as if funds are available and using the balance in the accounts for expenditures.
e	Commercial Loan Fraud	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/ 657 - Embezzlement, Theft or Misapplication of Funds	A fraudulent loan involving a corporation, commercial enterprise, or other type of business, usually secured by some form of collateral. One example includes banks advancing loan funds to car dealers via floor plan lines of credit secured by the automobiles in inventory. Collateral is or later sold, out of trust, and proceeds are not applied to the loan thus creating a loss to the lender.
f	Computer Intrusion	18 U.S.C. Section 1030	A person who gains access to a computer system of a financial institution to: - Computer Fraud * Remove, steal, procure or otherwise affect funds of the institution or the institution's customers * Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or * Damage, disable or otherwise affect critical systems of the institution. Note: Does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information See Issue 3, page 15, of *The SAR Activity Review* for additional information on Computer Intrusion at the following hyperlink: http://www.fincen.gov/sarreviewissue3.pdf.

© gettechnical inc 2021

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statutes	Explanation/Description
g	Consumer Loan Fraud	18 U.S.C. Section 1344- Bank Fraud18 U.S.C. Section656/657 - Embezzlement, Theft or Misapplication of Funds	A loan extended to an individual for personal or household use that is obtained fraudulently. Incidents of consumer loan fraud primarily involve the submission of false or forged by loan applicants.
h	Counterfeit Check	18 U.S.C. Section 1344- Bank Fraud	A legitimate check that is altered or forged by hand or through the use of a computer or electronic/digital device that is compromised or scanned into a computer. The payee's name, dollar amount, check serial number, and date are changed though other data (including the authorized signature) remain as they appear on the original check. The counterfeit check is purported to be genuine and negotiated
I	Counterfeit Credit/Debit Card	18 U.S.C. Section 1029- Fraud and Related Activity in Connection with Access Device18 U.S.C. Section 1344 - Bank Fraud	A person who knowingly commits fraud by producing, using, or selling one or more counterfeit credit or debit cards. A counterfeit or fake card is created through technology to emboss stolen or fictitious card numbers, along with hologram and card issuer images, and magnetic stripes on white plastic. The cards are used for fraudulent purchases or sold to other criminals for their use.
j	Counterfeit Instrument	18 U.S.C. Section 1344- Bank Fraud	The manufacture, copy, reproduction, or forgery of an instrument with the intent to defraud a financial institution. Instruments could include notes, checks, securities, bonds, certificates and other negotiable financial instruments.
k	Credit Card Fraud	18 U.S.C. Section 1344- Bank Fraud	The intentional procurement of goods, services or money, without the authorization of the cardholder, credit card member or its agent, by using a stolen, lost, or cancelled credit card. May include Illegal purchases made in person, via the Internet or telephone, or through cash advances

© gettechnical inc 2021

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statutes	Explanation/Description
l	Debit Card Fraud	18 U.S.C. Section 1344- Bank Fraud	The unauthorized use of a stolen, lost, or cancelled debit card for payment of goods or to acquire services or money. Debit cards are used in place of checks or cash and usually are tied to a checking account. Fraudulent use of the debit card depletes available funds in that account causing a loss to the bank customer or to the bank.
m	Defalcation/ Embezzlement	18 U.S.C. Section 656/657- Theft, Embezzlement or misapplication of funds	A person who, for unauthorized personal use, embezzles, abstracts, purloins or willfully, misapplies any of the moneys, funds or credits of a bank, branch, agency or organization or holding company or any moneys, funds, assets or, securities entrusted to the custody or care of such bank, branch, agency, organization, or holding company.
n	False Statement	18 U.S.C. Section 1001- False Statements or entries 18 U.S.C. Section 1005- False Entries 18 U.S.C. Section 1014- False Statements on a Loan or Credit Application	A person who knowingly and willfully commits one of the following: 1. Falsifies, conceals or covers up by any trick, scheme or device, a material fact 2. Makes any materially false, fictitious or fraudulent statement or representation; or 3. Makes or uses any false writing or document knowing the same to contain any materially false, fictitious or fraudulent statement or entry. The false statement must occur in a matter within the jurisdiction of a branch of the United States Government; essentially, making a false statement to a government agency when it is carrying out its mission. Section covers oral or written false statements or misrepresentations made knowingly on a loan or on a or credit application to an insured bank (e.g., willful over-valuing of land, property, securities, or other assets or the understatement of liabilities). Such statements or misrepresentations must have been capable of influencing the bank's credit decision. Actual damage or reliance on such information is not an essential element of the offense. The statute applies to credit renewals, continuations, extensions or deferments and includes willful omissions as well as affirmative false statements. Obsolete information in the original loan application is not covered unless the applicant reaffirms the information in connection with a renewal request. The application will trigger the statute even if the loan is not made.

© gettechnical inc 2021

o	Misuse of Position / Self Dealing	18 U.S.C. Section 656/657- Theft, Embezzlement or Misapplication of Funds 18 U.S.C. Section 644 - Banker Receiving Unauthorized Deposit of Public Money 18 U.S.C. Section 215 - Bank Bribery	A person, who is not an authorized depositary of public moneys, who knowingly receives from , any disbursing officer, collector of internal revenue, or other agent of the United States, public money on deposit, or by way of a loan or accommodation, with or without interest, or otherwise than in payment of a debt against the United States, or uses, transfers, converts, appropriates, or applies any portion of the public money for any purpose not prescribed by law.
p	Mortgage Loan Fraud	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657 - Theft, Embezzlement, or Misapplication of Funds	A person who fraudulently obtains a mortgage for property or other asset primarily by the submission of false or forged statements on loan applications.
q	Mysterious Disappearance	18 U.S.C. Section 656/657 - Theft, Embezzlement, or Misapplication of funds	Unexplained disappearance of moneys, or other instruments of value, in bearer form, from a financial institution's branch, agency, organization, or holding company.
r	Wire Transfer Fraud	18 U.S.C. Section 1956- Laundering of Monetary Instruments 18 U.S.C. Section 1343 - Fraud by Wire, Radio or Television	A person who, intending to defraud or obtain money or property by fraudulent means of false pretenses, representations or promises, transmits an electronic funds transfer.

© gettechnical inc 2021

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statutes	Explanation/Description
s	Other		A category used to report suspicious activity that does not fit into any other violations characterization.
t	Terrorist Financing	18 U.S.C. 2339(a) and 18 U.S.C. 2339(b) - Harboring and Concealing Terrorists	Persons or entities who provide material support or resources to various enumerated terrorist acts, including concealing or disguising the nature, location, source or ownership of the material support or resources. Also, persons or entities providing material support or resources to designated foreign terrorist organizations, or attempting or conspiring to do so. The statute explicitly provides for extraterritorial jurisdiction, meaning it can be applied to actions occurring outside the United States.
u	Identity Theft	18 U.S.C. Section 1028 - Identity Theft	A person who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under applicable state or local law. See Issue 2, page 14 of *The SAR Activity Review* for further details about identity theft at the following hyperlink: http://www.fincen.gov/sarreview2issue4web.pdf

© gettechnical inc 2021

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). The bank should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. When the bank uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions. Banks should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision will be based on unique facts and circumstances, no single form of documentation is required when a bank decides not to file.[4]

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[5]

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the federal banking agencies. FinCEN's guidelines suggest that banks should report continuing suspicious activity by filing a report at least every 90 days.[6] This practice will notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice will remind the bank that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as bank management determining that it is

[4] Bank Secrecy Act Advisory Group, "Section 4 — Tips on SAR Form Preparation & Filing," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 38, at www.fincen.gov.
[5] Refer to Interagency Enforcement Statement (Appendix R) for additional information.
[6] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 1, October 2000, page 27 at www.fincen.gov.

© gettechnical inc 2021

necessary to terminate a relationship with the customer or employee that is the subject of the filing.

Banks should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that a bank maintain a particular account, the bank should ask for a written request. The written request should indicate that the agency has requested that the bank maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by a bank in accordance with its own standards and guidelines.[7]

The bank should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts. The procedures should include:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
- Criteria for when analysis of the overall customer relationship is necessary.
- Criteria for whether and, if so, when to close the account.
- Criteria for when to notify law enforcement, if appropriate.

SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SAR forms are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. Beginning on September 12, 2009, banks that file SARs electronically can receive from FinCEN a Document Control Number as an acknowledgement of receipt for a submitted SAR.[8]

Timing of a SAR Filing

The SAR rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.[9]

---

[7] Refer to *Requests by Law Enforcement for Financial Institutions to Maintain Accounts,* June 13, 2007, at www.fincen.gov.
[8] Refer to http://fincen.gov/whatsnew/html/20090826.html for additional information.
[9] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review – Trends, Tips & Issues*, Issue 1, October 2000, page 27, at www.fincen.gov.

© gettechnical inc 2021

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The bank's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation.[10]

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that a bank has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.[11]

For situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the bank's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.[12]

Notifying Board of Directors of SAR Filings

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties.[13]

---

[10] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 44, at www.fincen.gov. For examples of when the date of initial detection occurs, refer to *SAR Activity Review — Trends, Tips, and Issues,* Issue 14, October 2008, page 38 at www.fincen.gov.

[11] *Id.*

[12] For suspicious activity related to terrorist activity, institutions may also call FinCEN's Financial Institution's terrorist hotline at the toll free number 866-556-3974 (7 days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

[13] As noted in the Bank Secrecy Act Advisory Group's *The SAR Activity Review — Trends, Tips & Issues*, Issue 2, June 2001, "In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an

© gettechnical inc 2021

SAR Record Retention and Supporting Documentation

Banks must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. Additionally, banks must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all documents or records that assisted a bank in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or federal banking agency.[14]

Prohibition on Disclosures by Financial Institutions:

Federal law (31 U.S.C. 5318(g)(2)) provides that a financial institution, and its directors, officers, employees, and agents who, pursuant to any statutory or regulatory authority or on a voluntary basis, report suspicious transactions to the government, may not notify any person involved in the transaction that the transaction has been reported. Provided that no person involved in the suspicious activity is notified, 31 CFR Chapter X clarifies that the following activity does not constitute a prohibited disclosure:

• Disclosure of SAR information to certain governmental authorities or other examining authorities that are otherwise entitled by law to receive SAR information or to examine for or investigate suspicious activity;

• Disclosure of the underlying facts, transactions, and documents upon which a BSA SAR is based; and

• For those institutions regulated by a Federal functional regulator (Federal bank regulatory agencies, the Securities and Exchange Commission (SEC), and the

Commodity Futures Trading Commission (CFTC)), the sharing of SAR information within an institution's corporate organizational structure, for purposes that are consistent with the Bank Secrecy Act, as determined by regulation or guidance.

individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised." Refer to www.fincen.gov.

[14] Refer to *Suspicious Activity Report Supporting Documentation,* June 13, 2007, at www.fincen.gov.

© gettechnical inc 2021

(c) Exceptions. A bank is not required to file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities with respect to which the bank files a report pursuant to the reporting requirements of 17 CFR 240.17f–1.

(d) Retention of records. A bank shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Supporting documentation shall be identified, and maintained by the bank as such, and shall be deemed to have been filed with the SAR. A bank shall make all supporting documentation available to FinCEN or any Federal, State, or local law enforcement agency, or any Federal regulatory authority that examines the bank for compliance with the Bank Secrecy Act, or any State regulatory authority administering a State law that requires the bank to comply with the Bank Secrecy Act or otherwise authorizes the State authority to ensure that the institution complies with the Bank Secrecy Act, upon request.

(e) Confidentiality of SARs. A SAR, and any information that would reveal the existence of a SAR, are confidential and shall not be disclosed except as authorized in this paragraph (e). For purposes of this paragraph (e) only, a SAR shall include any suspicious activity report filed with FinCEN pursuant to any regulation in this part.

(1) Prohibition on disclosures by banks.

(i) General rule. No bank, and no director, officer, employee, or agent of any bank, shall disclose a SAR or any information that would reveal the existence of a SAR. Any bank, and any director, officer, employee, or agent of any bank that is subpoenaed or otherwise requested to disclose a SAR or any information that would reveal the existence of a SAR, shall decline to produce the SAR or such information, citing this section and 31 U.S.C. 5318(g)(2)(A)(i), and shall notify FinCEN of any such request and the response thereto.

(ii) Rules of Construction. Provided that no person involved in any reported suspicious transaction is notified that the transaction has been reported, this paragraph (e)(1) shall not be construed as prohibiting:

(A) The disclosure by a bank, or any director, officer, employee, or agent of a bank, of:

(1) A SAR, or any information that would reveal the existence of a SAR, to FinCEN or any Federal, State, or local law enforcement agency, or any Federal regulatory authority that examines the bank for compliance with the Bank Secrecy Act, or any State regulatory authority administering a State law that requires the bank to comply with the Bank Secrecy Act or otherwise authorizes the State authority to ensure that

© gettechnical inc 2021

the bank complies with the Bank Secrecy Act; or

(2) The underlying facts, transactions, and documents upon which a SAR is based, including but not limited to, disclosures:

(i) To another financial institution, or any director, officer, employee, or agent of a financial institution, for the preparation of a joint SAR; or

(ii) In connection with certain employment references or termination notices, to the full extent authorized in 31 U.S.C. 5318(g)(2)(B); or

(B) The sharing by a bank, or any director, officer, employee, or agent of the bank, of a SAR, or any information that would reveal the existence of a SAR, within the bank's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act as determined by regulation or in guidance.

(2) Prohibition on disclosures by government authorities. A Federal, State, local, territorial, or Tribal government authority, or any director, officer, employee, or agent of any of the foregoing, shall not disclose a SAR, or any information that would reveal the existence of a SAR, except as necessary to fulfill official duties consistent with Title II of the Bank Secrecy Act. For purposes of this section, ''official duties'' shall not include the disclosure of a SAR, or any information that would reveal the existence of a SAR, in response to a request for disclosure of non-public information or a request for use in a private legal proceeding, including a request pursuant to 31 CFR 1.11.

(f) Limitation on liability. A bank, and any director, officer, employee, or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this section or any other authority, including a disclosure made jointly with another institution, shall be protected from liability to any person for any such disclosure, or for failure to provide notice of such disclosure to any person identified in the disclosure, or both, to the full extent provided by 31 U.S.C. 5318(g)(3).

(g) Compliance. Banks shall be examined by FinCEN or its delegatees for compliance with this section. Failure to satisfy the requirements of this section may be a violation of the Bank Secrecy Act and of this part. Such failure may also violate provisions of Title 12 of the Code of Federal Regulations.

© gettechnical inc 2021

SHARING SARS WITH HEAD OFFICES AND CONTROLLING COMPANIES

Interagency guidance clarifies that banking organizations may share SARs with head offices and controlling companies, whether located in the United States or abroad.[15] A controlling company as defined in the guidance includes:

- A bank holding company (BHC), as defined in section 2 of the BHC Act.
- A savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act.
- A company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an industrial loan company or parent company.

The guidance confirms that:

- A U.S. branch or agency of a foreign bank may share a SAR with its head office outside the United States.
- A U.S. bank may share a SAR with controlling companies whether domestic or foreign.

Banks should maintain appropriate arrangements to protect the confidentiality of SARs. The guidance does not address whether a bank may share a SAR with an affiliate other than a controlling company or head office. Therefore, banks should not share SARs with such affiliates. However, in order to manage risk across an organization, banks that file a SAR may disclose to entities within its organization the information underlying a SAR filing.

[15] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies*, issued by Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision, January 20, 2006.

© gettechnical inc 2021

Importance of SAR Reporting to Law Enforcement Investigations

Analysis of SARs plays a critical role in various types of law enforcement investigations. Regardless of the underlying crime, SARs serve as a vital tool for identifying and tracking funds derived from criminal activity. SAR data provides valuable pieces of information that are similar to pieces of a puzzle - each separate piece helps investigators identify complex and sophisticated relationships between people, businesses, locations and assets. Although it is sometimes impossible to obtain 100 percent of the information requested on SAR forms, a concerted effort to obtain specific "puzzle pieces" is very valuable to law enforcement.

Filers should strive to obtain and record as much suspect information as possible. When a suspect exists, always enter suspect related data in the appropriate "Suspect" portion of the form.

A recent review of filings indicates that some forms actually contain no identifying names for the suspect but rather have references such as "See Part V" or "See next Page" in the suspect portion of the form. This limits investigative capabilities used to identify suspects and to allow accurate data retrieval/query efforts by law enforcement. Using only a first initial rather than a full first name also poses problems in accurately identifying suspects.

Whenever possible, try to obtain complete first names for all suspects. Address information should contain street numbers and apartment numbers if known. Foreign countries should be entered using the attached database standardized country codes. Suspects' occupations also provide high quality leads for law enforcement investigators. When it is known, vital information should be captured in the suspect area of the SAR form.

Another critical piece of the puzzle is found in identification numbers. Passport numbers should reflect the country of issue in the "Issuing Authority" section using the standardized country codes. Alien registration numbers contain a letter of the alphabet preceding the actual number – always enter the letter along with the number.

A major element that increases the utility of SARs for law enforcement is the narrative information or "description of activity." If the activity involves wire transfer transactions, include destination city, state and country as well as names of banks and beneficiary persons or businesses. Of particular value are names of foreign financial institutions and the account numbers associated with funds transfers. The use of money orders, traveler's checks, foreign currency or other monetary instruments should also be noted within the activity description. If stocks, bonds, letters of credit, investments, commodities, etc. are involved, this should also be noted as this helps identify methodologies associated with criminal activities.

SAR filers who make reasonable efforts to obtain, record and report the key information outlined above will enhance the ultimate utility of SARs for law enforcement purposes.

© gettechnical inc 2021

Date of "Initial Detection" and the 30-Day SAR Clock

By FinCEN Office of Outreach Resources

This section of The SAR Activity Review discusses current issues raised with regard to the preparation and filing of SARs. This section is intended to identify suspicious activity reporting-related issues and provide meaningful guidance to filers. In addition, it reflects the collective positions of the government agencies that require organizations to file SARs.

Bank Secrecy Act suspicious activity reporting rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR .6 Upon identification of unusual activity, additional research is typically conducted and institutions may need to review customer transaction or account activity to determine whether to file a SAR. The need to review a customer's account activity, including transactions, does not necessarily indicate the need to file a SAR, even if a reasonable review of the activity or transaction might take an extended period of time. The time period for filing a SAR starts when the institution, in the course of its review or as a result of other factors, reaches the conclusion that it knows, or has reason to suspect, that the activity or transactions under review meets one or more definitions of suspicious activity.

Guidance on the timing of when a SAR must be filed was first set forth in the October 2000 SAR Activity Review: Tips, Trends & Issues (Issue 1).7 In May of 2006, FinCEN issued additional guidance in The SAR Activity Review: Tips, Trends & Issues (Issue 10)8 to clarify any ambiguity in the interpretation of the original guidance. Institutions continue to seek clarification about the phrase "initial detection", and so FinCEN is issuing additional guidance with examples that illustrate appropriate timing for filing a SAR.

As clarified in the May 2006 SAR Activity Review: Tips, Trends & Issues (Issue 10), the phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. A real estate investment (purchase or sale), or the receipt of an inheritance or gift, for example, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. An institution's automated account monitoring system or initial discovery of activity, such as system-generated reports, may flag the transaction for review; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under

© gettechnical inc 2021

review is “suspicious” within the meaning of the SAR regulations. Institutions may have implemented multi-layer review procedures and/or systems in order to better detect and report suspicious activity. FinCEN recognizes that these multi-layer review processes may involve such steps as a red flag notice from an account monitoring system, a brief review by an analyst, and an investigation by an investigator. For example, an institution may have implemented an automated red flag system that detects unusual patterns in transactions. It may then utilize an analyst as a first step in determining whether the red flag notice is an obvious “false positive” or whether the activity should be forwarded to an investigator. In this example, the analyst makes no formal determination as to whether the activity may be suspicious based on the unusual transaction pattern and instead refers the matter to an investigator. After a period of appropriate review, the investigator determines whether the activity is suspicious. Thus, the date of initial detection is the date when the investigator has appropriately reviewed the activity and makes a determination that it is suspicious, not when the analyst refers the matter to the investigator.

The following examples illustrate that the date of initial detection does not necessarily occur on the date of the transaction(s), the date when an automated system generates a notice or red flag alert, or the date when an employee initially reviews the transaction(s). The following examples assume that the monetary thresholds have been met per the SAR regulation applicable to the specific type of institution. Note: Institutions are reminded that reviews of suspicious activity should be completed in a reasonable period of time.9

Examples:

Example 1: A customer makes two deposits of $9,900 over the course of two business days. On the third day, an alert teller notifies the BSA analyst that the customer has made deposits of just below $10,000 two days in a row. The analyst makes a determination that the two deposits of $9,900 are most likely indicative of structuring and therefore, the transactions are suspicious. That same day, the analyst refers the matter to the investigator and notes that the transactions are suspicious and likely involve intent to structure transactions to avoid CTR reporting requirements. The date of initial detection in this example is the date when the analyst was able to make a determination that the activity is suspicious. The institution has 30 days to file a SAR from the date of the analyst’s determination.

Example 2: An import/export business customer suddenly begins sending and receiving large wire transfers from high risk jurisdictions. The institution’s automated account monitoring system generates a red flag notification to the BSA officer, who conducts an initial review of the transactions. Given the complexity of the customer’s business, the BSA officer is not in a position to determine whether the transactions may be suspicious. The officer refers the information to the institution’s SAR investigator, who spends several days reviewing the customer’s transactions and researching the nature of the customer’s import/export business. After ten days of research, the investigator is able to make a determination that the activity does not appear to have a business or lawful purpose, and, therefore, the activity is suspicious. The day on which the investigator makes such a determination should be considered the date of the initial detection, and the institution has 30 days from that date to file a SAR.

© gettechnical inc 2021

Example 3: An individual purchases money orders at several agent locations of an institution within the same city on the same business day. The next day, the institution's software system alerts the BSA assistant to the pattern of transactions. The assistant reviews the transactions and determines that transactions should be reviewed by the institution's BSA officer. The officer commences a review and a few days later the officer identifies another series of transactions conducted by the individual but still does not have enough information to determine if the activity is suspicious. A week later, the individual initiates a wire transfer to a high risk jurisdiction and provides the agent's employee with alarming information during a conversation. The employee informs the BSA officer of the updated information, and the officer makes a determination that the activity is suspicious, that a SAR should be filed, and that law enforcement should be contacted immediately. From that date, the institution has 30 days to file a SAR.

© gettechnical inc 2021

INVESTIGATION WORKSHEET

Date of Investigation:_____ Date potential SAR went to committee_____

Source of Investigation:

- ☐ Incident Report from Employee (attached)
- ☐ System Generated Report (attached)
- ☐ New Account Opening (worksheet attached)
- ☐ Insider
- ☐ Law enforcement inquiry
- ☐ Public sources
- ☐ Other

Subject Name(s):

Activities involved:

Any loss to financial institution?

Committee decision:

- ☐ File SAR
- ☐ Continue to Observe behavior
- ☐ Do not file SAR

Reason for not filing SAR:_____

_____

_____

_____

_____

© gettechnical inc 2021

The following guidance is provided by the federal regulatory authorities and/or FinCEN.

Importance of having a Centralized Review of SARs

Financial institutions might consider establishing a centralized location for the review and processing of SARs. Nevertheless, as part of an institution's internal controls, it is especially important that adequate management review of the SAR contents and filing is completed before the SAR is submitted. If a centralized review process is employed, financial institutions should ensure that the identity of the bank, its primary regulator, and the location of the transaction are clearly indicated on the SAR and that the SAR is not filed under the name and location of the centralized processing unit.

Also, when appropriate, the financial institution may wish to seek legal counsel during the filing process.

New Depository Institution SAR Form—added terrorism and identity theft

FinCEN, in conjunction with the regulatory agencies, has amended the Depository Institution SAR form (Form TD F 90-22.47) in order to include two new boxes, one for terrorism and one for identity theft.

With regard to instances of possible terrorism, identity theft and computer intrusions, it is recognized that the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file, nonetheless, in appropriate situations involving these matters, based on the potential harm that such crimes can produce. In addition, financial institutions are reminded that even when the dollar thresholds of the regulations are not met, the institutions have the discretion to file a SAR. In such situations, the financial institutions will still enjoy the safe harbor provided for in the statute.

With regard to identity theft, financial institutions should keep in mind that the victim's name should not go on the first page of the SAR under the field "suspect." If there is no identifiable suspect, that field should state "unknown." The victim's name should be stated in the "Narrative" section of the form.

Filling out the SAR Form

If the SAR is filled out at a centralized location within the financial institution or at the holding company level, it is extremely important that the SAR identify the actual financial institution involved, the location of the office or branch where the activity took place, and the correct primary federal regulator. (In situations where the holding company or an affiliate is filing the SAR, the primary federal regulator of the financial institution involved may not be the regulator of the holding company or the affiliate.)

© gettechnical inc 2021

With regard to the designation of the type of violation that is involved, financial institutions are strongly encouraged to use the "Other" box only when absolutely necessary, that is, when it is clear that none of the other available boxes is applicable. Overuse of the "Other" box distorts the data in the system and makes it more difficult to search for particular types of violations. A recent review of the SAR database indicated that there were many instances in which the "Other" box was checked when there were more applicable, specific boxes that should have been checked.

Closing of an Account

There is no requirement in the SAR regulations that a financial institution must close an account that is the subject of the filing of a SAR. The decision to maintain or close an account is left to the financial institution. However, if an account is involved in a suspicious or potentially illegal transaction, the institution should examine the status and history of the account thoroughly and should determine whether or not the institution is comfortable with leaving the account open. It is often advisable to include legal counsel in making this decision. If the institution is aware that the reported activity is under investigation, it is strongly recommended that the financial institution notify law enforcement before closing an account.

Contacting Law Enforcement

Financial institutions are reminded that in situations involving violations requiring immediate attention, such as when a reportable violation (e.g., money laundering scheme, terrorist financing, or other financial crime) is ongoing, the financial institution shall immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities. Also, remember that direct contact by telephone or in person with law enforcement and supervisory authorities to report possible suspicious activity does not relieve the institution from filing a timely SAR to the IRS DCC.

© gettechnical inc 2021

Guidance on when a SAR must be filed was first set forth in the October 2000 SAR Activity Review: Tips, Trends & Issues. We are issuing updated guidance on this topic to clarify ambiguity in the interpretation of the original guidance.

Our suspicious activity reporting rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR.[16] If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Upon identification of unusual activity, additional research is typically conducted, and institutions may need to review transaction or account activity for a customer to determine whether to file a SAR. The need to review a customer's account activity, including transactions, does not necessarily indicate the need to file a SAR, even if a reasonable review of the activity or transaction might take an extended period of time. The time period to file a SAR starts when the institution, in the course of its review or as a result of other factors, reaches the conclusion in which it knows, or has reason to suspect, that the activity or transactions under review meets one or more of the definitions of suspicious activity.[17]

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. A real estate investment (purchase or sale), the receipt of an inheritance, or a gift, for example, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The institution's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulations.

A review must be initiated promptly upon identification of unusual activity that warrants investigation. The timeframe required for completing review of the identified activity, however, may vary given the situation. According to the FFIEC's 2005 *Bank Secrecy Act/Anti-Money Laundering Examination Manual,*[18] "an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time."[19] What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR

[16] 31 C.F.R. § 1026.320; 31 C.F.R. § 1020.320; 31 C.F.R. § 1023.320; 31 C.F.R. § 1022.320; 31 C.F.R. § 1021.320
[17] BSA Advisory Group, "Section 5 – Issues and Guidance" *The SAR Activity Review-Trends, Tips & Issues,* October 2000, page 27.
[18] An electronic version of the *FFIEC BSA/AML Examination Manual* may be found at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.
[19] While the *FFIEC BSA/AML Examination Manual* is specific to the banking industry, this piece of guidance is also applicable to other industries with suspicious activity reporting requirements.

© gettechnical inc 2021

monitoring, reporting, and decision-making process of each institution. The key factor is that an institution has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.

For violations requiring immediate attention, in addition to filing a SAR, financial institutions should immediately notify law enforcement via telephone, and as necessary, their functional regulator. For suspicious activity related to terrorist activity, institutions may also call FinCEN's toll-free hotline at 1-866-556-3974 (7 days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

© gettechnical inc 2021

CONFIDENTIALITY

© gettechnical inc 2021

Federal law (31 U.S.C. 5318(g)(3)) provides financial institutions complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to a regulatory requirement or on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees, and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure."

Confidentiality of SARs:

A Bank Secrecy Act Suspicious Activity Report (BSA SAR), and any information that would reveal the existence of the BSA SAR (collectively, "SAR information"), are confidential, and may not be disclosed except as specified in 31 U.S.C. 5318(g)(2) and in FinCEN's regulations (31 CFR Chapter X).

Prohibition on Disclosures by Financial Institutions:

Federal law (31 U.S.C. 5318(g)(2)) provides that a financial institution, and its directors, officers, employees, and agents who, pursuant to any statutory or regulatory authority or on a voluntary basis, report suspicious transactions to the government, may not notify any person involved in the transaction that the transaction has been reported. Provided that no person involved in the suspicious activity is notified, 31 CFR Chapter X clarifies that the following activity does not constitute a prohibited disclosure:

- Disclosure of SAR information to certain governmental authorities or other examining authorities that are otherwise entitled by law to receive SAR information or to examine for or investigate suspicious activity;
- Disclosure of the underlying facts, transactions, and documents upon which a BSA SAR is based; and
- For those institutions regulated by a Federal functional regulator (Federal bank regulatory agencies, the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC)), the sharing of SAR information within an institution's corporate organizational structure, for purposes that are consistent with the Bank Secrecy Act, as determined by regulation or guidance.

Prohibition on Disclosures by Government Authorities:

Federal law (31 U.S.C. 5318(g)(2)) also provides that an officer or employee of any

© gettechnical inc 2021

Federal, state, local, tribal, or territorial government within the United States who has knowledge that such report was made, may not disclose to any person involved in the transaction that the transaction has been reported, other than as necessary to fulfill the official duties of such officer of employee. FinCEN's regulations clarify that "official duties" must be consistent with Title II of the Bank Secrecy Act and shall not include the disclosure of a SAR, or any information that would reveal the existence of a SAR, in response to a request for disclosure of non-public information or a request for use in a private legal proceeding, including a request pursuant to 31 CFR § 1.11.

© gettechnical inc 2021

PROHIBITION ON NOTIFICATION

As set forth in the October 2000 *SAR Activity Review* (Section 5 - Disclosure of SARs and Underlying Suspicious Activity), federal law (31 U.S.C. 5318(g)(2)) prohibits the notification to any person that is involved in the activity being reported on a SAR that the activity has been reported.
This prohibition extends to disclosures that could indirectly result in the notification to the subject of a SAR that a SAR has been filed, effectively precluding the disclosure of a SAR or even its existence to any persons other than appropriate law enforcement and supervisory agency or agencies. Self-regulatory organizations such as the New York Stock Exchange and the National Association of Securities Dealers are not appropriate supervisory agencies under current law for purposes of SAR disclosure by financial institutions.

This prohibition does not preclude, under federal law, a disclosure in an appropriate manner of the facts that are the basis of the SAR, so long as the disclosure is not made in a way that indicates or implies that a SAR has been filed or that information is included on a filed SAR.
In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised.

The prohibition on notification of a SAR filing can raise special issues when SAR filings are sought by subpoena or court order. The SAR regulations direct organizations facing these issues to contact their primary supervisor, as well as FinCEN, to obtain guidance and direction on how to proceed. In several matters to date, government agencies have intervened to ensure that the protection for filing organizations and the integrity of the data contained within the SAR database remain intact.

Call Office of Chief Counsel at Fin CEN at (703) 905-3590

If a financial institution is served with any subpoena requiring disclosure of the fact that a SAR has been filed or of the Report itself, except to the extent that the subpoena is submitted by appropriate law enforcement or supervisory agency, the financial institution should neither confirm nor deny the existence of the SAR. You should immediately call the above number and your regulatory agency. SAR Bulletin Issue 9.

Disclosure of SAR Documentation

Under the SAR regulations, institutions filing SARs should identify within the SAR, and are directed to maintain all "supporting documentation" related to the activity being reported. Disclosure of supporting documentation related to the activity that is being reported on a

© gettechnical inc 2021

SAR does not require a subpoena, court order, or other judicial or administrative process. Under the SAR regulations, financial institutions are required to disclose supporting documentation to appropriate law enforcement agencies, or FinCEN, upon request.

In SAR Bulletin Issue 9, October 2005 this subject was discussed in greater detail. Disclosures to requests from FinCEN or appropriate law enforcement and regulatory agencies do not undermine the safe harbor provisions. Financial institutions should take special care to verify that a requestor of information is a representative of one of these groups. Procedures should be incorporated into the AML program.

Examples of those who can receive supporting documentation include:

- Criminal investigative Services of Armed Forces
- The Bureau of Alcohol, Tobacco, and Firearms
- Attorney General
- District Attorney
- State's attorney
- Drug Enforcement Administration
- The Federal Bureau of Investigation
- Internal Revenue Service
- Tax Enforcement agencies at state level
- Office of Foreign Assets Control
- State or local police department
- US Attorney
- Immigration and customers Enforcement
- US Postal Inspection Service
- U S Secret Service

Financial institutions are required to disclose documentation supporting the filing of a Suspicious Activity Report to an appropriate federal or state regulatory/supervisory agency upon request. In addition, financial institutions may share a SAR, or information contained in it, with an appropriate with an appropriate supervisory or regulatory agency.

Call 800-949-2732 for help.

Applicability of Safe Harbor

The safe harbor provisions applicable to SAR filings provide a safe harbor for organizations that provide a SAR to all authorized government personnel, including Federal, state, and local authorities. Similarly, the safe harbor provisions apply even if the report of activity that is a possible violation of law or regulation is made orally or in some form other than through the use of a SAR.

© gettechnical inc 2021

What should a financial institution do if it receives a civil subpoena that specifically asks for the production of Suspicious Activity Reports or a subpoena that, by virtue of its breadth, would encompass Suspicious Activity Reports?

If the subpoena does not specifically ask for the production of Suspicious Activity Reports, the financial institution should object to the subpoena on the grounds that some of its responsive material consists of confidential supervisory information.

If the subpoena does specifically ask for the production of Suspicious Activity Reports, the simple answer for the financial institution is to send the issuer of the subpoena a written objection referring to the regulations that have been promulgated by FinCEN and the federal regulatory agencies that state that all Suspicious Activity Reports are confidential and cannot be released.[36] For example, as set forth in the Office of the Comptroller of the Currency's regulation:

"SARs are confidential. Any national bank or person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing this section, applicable law (e.g., 31 U.S.C. 5318(g)), or both, and shall notify the OCC."

12 C.F.R. § 21.11(k).[37] A similar prohibition on disclosure is found in all FinCEN's Suspicious Activity Report regulations.[38] Accordingly, in addition to the suggested response above, when a financial institution receives a discovery request or a subpoena asking for the production of a Suspicious Activity Report, it should contact its primary federal regulatory agency and FinCEN (note: 31 C.F.R. 1020.320(e) requires banks to notify FinCEN if they receive a subpoena covering Suspicious Activity Reports), if it is a federally-regulated bank, or FinCEN, if it is any other type of financial institution. The agencies can usually work with the institution in crafting an appropriate response. The institution should also refer to the applicable regulations, refuse to disclose any Suspicious Activity Report and, similarly, refuse to disclose whether or not a Suspicious Activity Report exists. The financial institution and its lawyer should also be careful not to disclose the existence of a Suspicious Activity Report in a response to the subpoena. Rather, the privilege log or other responsive pleading should refer generically to "nonpublic supervisory information" or something similar in nature, and not to the Suspicious Activity Report itself.

Not only does Federal law prohibit the disclosure of Suspicious Activity Reports, but 31 U.S.C. § 5318(g), as amended, provides a safe harbor from civil liability for financial institutions that disclose possible violations of law or regulation, whether the disclosures are made by filing Suspicious Activity Reports, or are made voluntarily, with the appropriate government authority.

© gettechnical inc 2021

On May 24, 2004, an Interagency Advisory was issued by the five federal regulatory agencies and FinCEN to inform financial institutions about a recent federal court case, *Whitney Nat'l Bank* v. *Karam,* 306 F. Supp.2d 678 (S.D. Tex. 2004), that reaffirms the scope of the statutory "safe harbor" protections. While the *Whitney* court ruled in a case involving a national bank and the rules and regulations of the Office of the Comptroller of the Currency, the five federal regulatory agencies and FinCEN believe that the court's rulings apply to all financial institutions that file Suspicious Activity Reports in accordance with suspicious activity reporting rules. This advisory may be found at http://www.fincen.gov/advis35.pdf and we suggest that all financial institutions familiarize themselves with the information contained therein.

On occasion, the federal banking agencies and FinCEN have filed an amicus brief or letter to the court to assist a bank that is contesting the issuance of a subpoena requiring the production of a Suspicious Activity Report. Consequently, when a financial institution is in a position of contesting such a subpoena, it should contact FinCEN and, where applicable, the banking agencies as soon as possible for further guidance.

© gettechnical inc 2021

Banks should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects, identifying unusual or suspicious activity related to those subjects, and filing, as applicable, SARs related to those subjects. Law enforcement inquiries and requests can include criminal subpoenas, national security letters (NSLs), and section 314(a) requests.

Mere receipt of any law enforcement inquiry, does not, by itself, require the filing of a SAR by the bank. Nonetheless, a law enforcement inquiry may be relevant to a bank's overall risk assessment of its customers and accounts. It is incumbent upon a bank to assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program. The bank should determine whether a SAR is filed based on all customer information available.

© gettechnical inc 2021

Filing SARs on Continuing Activity after Law Enforcement Contact

Questions have been raised regarding the necessity for the continued filing of SARs on continuing activity after law enforcement has contacted a financial institution with regard to a SAR filing. In some instances, after the filing of one or more SARs, law enforcement has contacted a financial institution requesting more specific information with regard to the suspect activity or requesting identified supporting documentation. In other instances, a law enforcement agency has contacted a financial institution to report that it does not intend to investigate the matter reported on the SAR.

If conduct continues for which a SAR has been filed, the guidance set forth in the October 2000 *SAR Activity Review* (Section 5 - Repeated SAR Filings on the Same Activity) should be followed even if a law enforcement agency has declined to investigate or there is knowledge that an investigation has begun. The filing of SARs on continuing suspicious activity provides useful information to law enforcement and supervisory authorities. Moreover, the information contained in a SAR that one law enforcement agency has declined to investigate may be of interest to other law enforcement agencies, as well as supervisory agencies.

© gettechnical inc 2021

FINCEN ADVISORY: SAR CONFIDENTIALITY REMINDER FOR INTERNAL AND EXTERNAL COUNSEL OF FINANCIAL INSTITUTIONS (ISSUED 3/2/12)

Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2012-A002
Issued: March 2, 2012
Subject: SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to remind financial institutions, and in particular, the lawyers that advise them, of the requirement to maintain the confidentiality of Suspicious Activity Reports (SARs). FinCEN is concerned that an increasing number of private parties, who are not authorized to know of the existence of filed SARs, are seeking SARs from financial institutions for use in civil litigation and other matters. Financial institutions, and their current and former directors, officers, employees, agents, and contractors, are prohibited from disclosing SARs, or any information that would reveal the existence of a SAR.[1] FinCEN recognizes that an escalation in the number of requests for use of SARs in private litigation may increase the likelihood of an unauthorized disclosure of a SAR. This is especially true when external counsel is unfamiliar with the regulations covering SAR confidentiality. Financial institutions, and their current and former directors, officers, employees, agents, and contractors could be subject to civil and criminal penalties for the unauthorized disclosure of a SAR.

FinCEN is responsible for both safeguarding the information it collects under its regulations implementing the Bank Secrecy Act, including SARs, and promoting appropriate protection of this by authorized users of the data across the Federal, State and local levels of government. The unauthorized disclosure of SARs could undermine ongoing and future investigations by tipping off suspects, deterring financial institutions from filing SARs, and threatening the safety and security of institutions and individuals who file such reports. Such disclosure of SARs compromises the essential role SARs play in protecting our financial system and in preventing and detecting financial crimes and terrorist financing. The success of the SAR reporting system depends upon the

[1] *See* 31 CFR §§ 1020.320(e), 1021.320(e), 1022.320(d), 1023.320(e), 1024.320(d), 1025.320(e), and 1026.320(e), *see also* Pub. L. 112-74: Consolidated Appropriations Bill, Division C, Title I, Section 118 a*mending* 31 U.S.C. § 5318(g)(2)(A)(December 23, 2011).

© gettechnical inc 2021

financial sector's confidence that these reports will be appropriately protected.

Possible Civil and Criminal Penalties for Unauthorized SAR Disclosures

The unauthorized disclosure of a SAR is a violation of federal law.[2] Both civil and criminal penalties may be imposed for SAR disclosure violations. Violations may be enforced through civil penalties[3] of up to $100,000 for each violation and criminal penalties[4] of up to $250,000 and/or imprisonment not to exceed five years.[5] In addition, financial institutions could be liable for civil money penalties resulting from anti-money laundering program deficiencies (i.e., internal controls, training, etc.) that led to the SAR disclosure. Such penalties could be up to $25,000 per day for each day the violation continues.[6] FinCEN is committed to working with regulatory agencies, law enforcement, SROs, and financial institutions to take appropriate action for unauthorized disclosures of SARs. Incidents involving possible unauthorized SAR disclosures are investigated, and appropriate action is taken for violations of the law.

Guidance on Maintaining SAR Confidentiality

FinCEN reminds financial institutions to be vigilant in maintaining the confidentiality of SARs. This includes ensuring all employees, agents, and individuals appropriately entrusted with information in a SAR are informed of the individual obligation to maintain SAR confidentiality. This obligation applies not only to the SAR itself, but also to information that would reveal the existence (or non-existence) of the SAR. Likewise, such persons should be informed of the consequences for failing to maintain such confidentiality, which could include civil and criminal penalties as explained herein.

A financial institution may consider including such information as part of its ongoing training of all employees. Furthermore, financial institutions may want to remind their counsel of the strict requirements of SAR confidentiality. Additional risk-based measures to enhance the confidentiality of SARs could include, among other appropriate security measures, limiting access on a "need-to-know" basis, restricting areas for reviewing SARs, logging of access to SARs, using cover sheets for SARs or information that reveals the existence of a SAR, or providing electronic notices that highlight confidentiality concerns before a person may access or disseminate the information.

If you or your institution becomes aware of an unauthorized disclosure of a SAR, or if your institution receives a subpoena or other request for a SAR from other than an authorized government authority or self-regulatory organization as defined in the applicable SAR regulations, you should immediately contact FinCEN's Office of Chief Counsel at (703) 905-3590.[7] Additionally, an institution may be required to contact its primary federal regulator, as may be applicable in a corresponding SAR rule.

Questions or comments regarding the contents of this Advisory should be addressed to

---

[2] 31 U.S.C. §§ 5318(g)(2), 5321, and 5322.
[3] 31 U.S.C. § 5321 and 31 CFR § 1010.820.
[4] 31 U.S.C. § 5322 and 31 CFR § 1010.840.
[5] 31 U.S.C. § 5322(b) and 31 CFR § 103.59(c) (Criminal penalties may increase if the violation is committed while violating another law of the United States or as part of a pattern of illegal activity).
[6] 31 U.S.C. § 5321(a)(1).
[7] 31 CFR §§ 1020.320(e), 1021.320(e), 1022.320(d), 1023.320(e), 1024.320(d), 1025.320(e), and 1026.320(e).

© gettechnical inc 2021

the FinCEN Regulatory Helpline at 800-949-2732. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

© gettechnical inc 2021

Department of the Treasury
Financial Crimes Enforcement Network

Guidance

FIN-2007-G003
Issued: June 13, 2007
Subject: Suspicious Activity Report Supporting Documentation

The Financial Crimes Enforcement Network (FinCEN)[1] is issuing this guidance to clarify:

(1) The Bank Secrecy Act (BSA) requirement that financial institutions provide Suspicious Activity Report (SAR) supporting documentation in response to requests by FinCEN and appropriate law enforcement or supervisory agencies;[2]

(2) What constitutes "supporting documentation" under SAR regulations;[3] and

(3) When legal process is required for disclosure of supporting documentation.

(1) Disclosure of Supporting Documentation to FinCEN and Appropriate Law Enforcement or Supervisory Agencies

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[4] Financial institutions must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement[5] or supervisory agency.[6]

When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or anti-money laundering program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

Disclosure of SARs to appropriate law enforcement and supervisory agencies is protected by the safe harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions.[7]

(2) What Constitutes Supporting Documentation

© gettechnical inc 2021

"Supporting documentation" refers to all documents or records that assisted a financial institution in making the determination that certain activity required a SAR filing. A financial institution must identify supporting documentation at the time the SAR is filed,[8] and this documentation must be maintained by the institution as such. The manner in which a financial institution maintains supporting documentation may vary from institution to institution, but each institution should prescribe its own method in its anti-money laundering program written procedures. For instance, a financial institution's procedures may require that all supporting documentation for a particular SAR be segregated in a single file folder or scanned and maintained in a data file.

What qualifies as supporting documentation depends on the facts and circumstances of each filing. As indicated in each of the SAR forms, financial institutions should identify in the SAR narrative the supporting documentation, which may include, for example, transaction records, new account information, tape recordings, e-mail messages, and correspondence. While items identified in the narrative of the SAR generally constitute supporting documentation, a document or record may qualify as supporting documentation even if not identified in the narrative.

(3) No Legal Process is Required for Disclosure of Supporting Documentation

The Right to Financial Privacy Act (RFPA) generally prohibits financial institutions from disclosing a customer's financial records to a Government agency without service of legal process, notice to the customer and an opportunity to challenge the disclosure.[9] However, no such requirement applies when the financial institution provides the financial records or information to FinCEN or a supervisory agency in the exercise of its "supervisory, regulatory or monetary functions."[10] In addition, no such requirement applies when FinCEN or an appropriate law enforcement or supervisory agency requests either a copy of a SAR or supporting documentation underlying the SAR.

With respect to supporting documentation, rules under the BSA state explicitly that financial institutions must retain copies of supporting documentation, that supporting documentation is "deemed to have been filed with" the SAR, and that financial institutions must provide supporting documentation upon request.[11] FinCEN has interpreted these regulations under the BSA as requiring a financial institution to provide supporting documentation even in the absence of legal process. FinCEN understands that this is in accord with the RFPA, which states that nothing in the act "authorize(s) the withholding of financial records or information required to be reported in accordance with any Federal statute or rule promulgated thereunder."[12]

[1]FinCEN consulted with staffs of the Department of Justice, the Federal Bureau of Investigation, the Internal Revenue Service's Criminal Investigation Division, the United States Secret Service, the Department of Homeland Security's Immigration and Customs Enforcement, the Drug Enforcement Administration, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, the Commodity Futures Trading Commission, and the Securities and Exchange Commission prior to issuing this guidance.
[2]*See* 31 C.F.R. § 1024.320(c); 31 C.F.R. § 1025.320(e); 31 C.F.R. § 1026.320(d); 31 C.F.R. § 1020.320(d); 31 C.F.R. § 1023.320(d); 31 C.F.R. § 1022.320(c); and 31 C.F.R. § 1021.320(d).
[3]*Id.*
[4]*Id.*
[5]*See "Providing Suspicious Activity Reports to Appropriate Law Enforcement,"* SAR Activity Review: Trends, Tips & Issues, Issue 9 (Oct. 2005), p.43, http://www.fincen.gov/sarreviewissue9.pdf.

[6] Supervisory agencies have independent statutory authority to examine all books and records of the financial institutions for which they are the appropriate regulator.
[7] The BSA provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are mandatory. Specifically, the BSA provides that a financial institution, or a director, officer, employee, or agent of a financial institution, that makes a "voluntary disclosure of any possible violation of law or regulation to a government agency" shall not be liable to any person under "any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." 31 U.S.C. § 5318(g)(3).
[8] Suspicious Transactions Reporting Requirements, 61 Fed. Reg. 4326, 4330 (February 5, 1996). Supporting documentation should **not** be attached to the SAR filing.
[9] This guidance is only applicable to financial records or information that constitute supporting documentation pursuant to provisions in the Bank Secrecy Act that govern the reporting of suspicious transactions. Consequently, nothing in this guidance is intended to alter or modify the duties or obligations of financial institutions subject to the Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.), 18 U.S.C. § 1510, or similar provisions of law. When responding to law enforcement requests for customer financial records or information other than SAR supporting documentation, financial institutions subject to the RFPA must still comply with that statute's notice and challenge provisions in the absence of an applicable exception, e.g. service of a grand jury subpoena or a national security letter.
[10] *See* 12 U.S.C. § 3413(b).
[11] *See* 31 C.F.R. § 1024.320(c); 31 C.F.R. § 1025.320(e); 31 C.F.R. § 1026.320(d); 31 C.F.R. § 1020.320(d); 31 C.F.R. § 1023.320(d); 31 C.F.R. § 1022.320(c); and 31 C.F.R. § 1021.320(d).
[12] *See* 12 U.S.C. 3413(d).

Filing SARs on Activity outside the United States

Consistent with the SAR regulations, it is expected that financial institutions will file SARs on activity deemed to be suspicious even when a portion of the activity occurs outside of the United States or the funds involved in the activity originated from outside the United States. Although foreign-located operations of U.S. organizations are not required to file SARs, an organization may wish, for example, to file a SAR with regard to suspicious activity that occurs outside of the United States that is so egregious that it has the potential to cause harm to the entire organization. (It is, of course, expected that foreign-located operations of U .S. organizations that identify suspicious activity will report such activity consistent with local reporting requirements in the foreign jurisdiction where the operation is located.)

© gettechnical inc 2021

How Do I . . .?

In addition to the publication of the guidance packages in the Fall 2003, every previous issue of *The SAR Activity Review* includes tips on how to properly prepare Suspicious Activity Report forms. Following is a listing of some of those past topics.

Topic	Issue	Page	Hyperlink Address
Reporting Computer Intrusion and Frequently Asked Questions	3	38	http://www.fincen.gov/sarreviewissue3.pdf
Filing a Corrected or Amended Suspicious Activity Report	4	42	http://www.fincen.gov/sarreview082002.pdf
Filing a Suspicious Activity Report for Ongoing or Supplemental Information	4	43	http://www.fincen.gov/sarreview082002.pdf
Reporting Identity Theft and Pretext Calling	3	41	http://www.fincen.gov/sarreviewissue3.pdf
Importance of Accurate and Complete Narratives	5	55	http://www.fincen.gov/sarreviewissue5.pdf
Improvements to Eliminate Reporting Deficiencies	6	49	http://www.fincen.gov/sarreviewissue6.pdf
Informal Value Transfer System—Special Suspicious Activity Report Form Completion Guidance	5	57	http://www.fincen.gov/sarreviewissue5.pdf
Instructions for Completing the Suspicious Activity Report Form	6	50	http://www.fincen.gov/sarreviewissue6.pdf
Suspicious Activity Report Filing Tips for Money Services Businesses	4	42	http://www.fincen.gov/sarreview082002.pdf
Suspicious Activity Report Form Preparation and Filing	1	24	http://www.fincen.gov/sarreviewforweb.pdf
Suspicious Activity Report Forms: Where to Send Completed Suspicious Activity Report Forms	6	57	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist-Related Activity: How to report potential terrorist-related activity	6	53	http://www.fincen.gov/sarreviewissue6.pdf
Tips from the Regulators	6	54	http://www.fincen.gov/sarreviewissue6.pdf

© gettechnical inc 2021

OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

The Office of Foreign Asset Control (OFAC), among other things, provides financial institutions with instructions regarding the freezing and blocking of funds related to individuals and entities on OFAC's Specially Designated Nationals List. For information or guidance required in connection with OFAC, including information regarding the Specially Designated Nationals List, financial institutions should contact OFAC at its hotline (1-800-540-6322) or on-line at www.treas.gov/ofac.

Filing SARs on OFAC List or 314(a) Matches

A verified match with an entity on an OFAC list that involves funds in an amount above the applicable SAR filing threshold should trigger a SAR filing requirement. Any transaction with, by or for a person listed by OFAC is unlawful. Therefore, when a financial institution verifies that it has a match with the OFAC list, it always will have identified at least a potential violation of law. It is important, however, to verify "hits" identified by a financial institution's OFAC filters to ensure that there is a true match, looking not only at the full name, but the address and any other identifiers that have been provided by OFAC, to avoid false positives for common names, which, we are informed, has been most prevalent in the Kingpin sanctions program. If a financial institution has any questions about its OFAC obligations and responsibilities, it should call the OFAC Hotline at (800) 540-6322.

In contrast, a match with a named subject issued pursuant to the Section 314(a) process does not automatically require the filing of a SAR. Section 314(a) requests seek to identify assets associated with a particular suspect. There may be nothing about the particular account or transaction found in response to a Section 314(a) request that is inherently illegal. A financial institution should review the account activity or transaction(s) relating to the named subject for suspicious activity, and, if appropriate, file a SAR predicated upon the totality of the circumstances and the account activity, in addition to reporting the Section 314(a) match to FinCEN.

© gettechnical inc 2021

NATIONAL SECURITY LETTERS (NSLS) AND SARS

1. Overview

National Security Letters are written investigative demands that can be issued by the Federal Bureau of Investigation in counterintelligence and counterterrorism investigations to obtain the following:

a. Telephone and electronic communications records from telephone companies and Internet Service Providers.
b. Information from credit bureaus, and
c. Financial Records from financial institutions. Financial records are an original, copy of, or information known to have been derived from, any record help by a financial institution pertaining to the customer's relationship with the financial institution.

National Security Letters can be issued by other federal government authorities for purposes of conduction foreign counter or positive-intelligence activities, certain protective funds, or intelligence or counter intelligence analyses related to international terrorism to obtain financial records from financial institutions.

NSLs are highly confidential. Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a bank files a SAR after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the bank. Questions regarding NSLs should be directed to the bank's local FBI field office.
Contact information for the FBI field offices can be found at www.fbi.gov.

WATCH OUT THIS IS A REQUEST LETTER ITEM!

___Make available copies of policies, procedures, and processes used to comply with all criminal subpoenas, including national security letters (NSLs), related to BSA.

© gettechnical inc 2021

LAW ENFORCEMENT INQUIRY LOG

DATE	SOURCE	REQUEST	VERIFIED	DELIVERY
May 1, 2012	IRS Criminal Investigative Division Officer Sharon Theriot	Written request SAR and supporting documentation for Sally Jane Smith	Called the local office through independent telephone number from yellow pages	May 5, 2012 Delivered SAR and supporting documentation

© gettechnical inc 2021

MISCELLANEOUS

© gettechnical inc 2021

ANSWERS TO FREQUENLTY ASKED QUESTIONS REGARDING SUSPICIOUS ACTIVITY REPORTING AND OTHER ANTI-MONEY LAUNDERING CONSIDERATIONS (1-19-2021)

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
National Credit Union Administration
Office of the Comptroller of the Currency

Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations

January 19, 2021

The Financial Crimes Enforcement Network (FinCEN), jointly with the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the Federal banking agencies), and in consultation with the staff of certain other federal functional regulators, is issuing answers to frequently asked questions (FAQs) regarding suspicious activity reports (SARs) and other anti-money laundering (AML) considerations for financial institutions covered by SAR rules.[1] The answers to these FAQs clarify the regulatory requirements related to SARs to assist such financial institutions with their compliance obligations, while enabling financial institutions to focus resources on activities that produce the greatest value to law enforcement agencies and other government users of Bank Secrecy Act (BSA) reporting. The answers to these FAQs neither alter existing BSA/AML legal or regulatory requirements, nor establish new supervisory expectations; they were developed in response to recent Bank Secrecy Act Advisory Group (BSAAG) recommendations, as described in more detail in FinCEN's Advance Notice of Proposed Rulemaking (ANPRM) on Anti-Money Laundering Program Effectiveness, published in September 2020.[2]

Question 1: Requests by Law Enforcement for Financial Institutions to Maintain Accounts

Can a financial institution maintain an account or customer relationship for which it has received a written "keep open" request from law enforcement, even though the financial institution has identified suspicious or potentially illicit activity?[3]

1. Financial institutions subject to SAR requirements include: Banks (31 CFR § 1020.320), Casinos and Card Clubs (31 CFR § 1021.320), Money Services Businesses (31 CFR § 1022.320), Brokers or Dealers in Securities (31 CFR § 1023.320), Mutual Funds (31 CFR § 1024.320), Insurance Companies (31 CFR § 1025.320), Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR § 1026.320), Loan or Finance Companies (31 CFR § 1029.320), and Housing Government Sponsored Enterprises (31 CFR § 1030.320).
2. *See* https://www.federalregister.gov/documents/2020/09/17/2020-20527/anti-money-laundering-program-effectiveness.
3. The response provided to this question clarifies current regulatory requirements. Under the recently-enacted Anti-Money Laundering Act of 2020, the Secretary of the Treasury is required to issue guidance on the required elements of a keep open request, which is forthcoming. *See* § 6306 of the Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6001 – 6511 (enacted as Division F of the National Defense Authorization Act for Fiscal Year 2021).

© gettechnical inc 2021

Yes. Law enforcement may have an interest in ensuring that certain accounts and customer relationships remain open notwithstanding suspicious or potential criminal activity in connection with the account. A financial institution may decide to maintain an account based on a written "keep open" request from a law enforcement agency, however, it is not obligated to do so. The written request should be specific and indicate both that the law enforcement agency has requested that the financial institution maintain the account, as well as the purpose and duration of the request.[4] Keeping such an account open as requested may be highly useful to law enforcement and may further efforts to identify and combat money laundering, terrorist financing, and other illicit financial activities.

A financial institution should not be criticized solely for its decision to maintain an account relationship at the request of law enforcement or for its decision to close the account. Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own policies, procedures, and processes. It may be useful for financial institutions to maintain documentation of "keep open" requests, including after a request has expired. If financial institutions keep such an account open as requested by law enforcement, they are still required to comply with all applicable BSA requirements, including requirements to conduct ongoing risk-based monitoring, and, as appropriate, file SARs,[5] including continuing activity SARs consistent with FinCEN guidance.[6]

Question 2: Receipt of Grand Jury Subpoenas/Law Enforcement Inquiries and SAR Filing

Should a financial institution file a SAR solely on the basis of receiving a grand jury subpoena or other law enforcement inquiries?

No. The receipt of a law enforcement inquiry, such as a grand jury subpoena, does not by itself indicate that the criteria requiring the filing of a SAR have been met. However, receipt of a grand jury subpoena or other law enforcement inquiry is pertinent information relevant to a financial institution's overall assessment of risk and the risk profile for the relevant customer(s) and account(s). Generally, a financial institution will assess and review all relevant information it has about a customer that is the subject of a grand jury subpoena or other law enforcement inquiries, in accordance with its risk-based AML program. For example, the receipt of a grand jury subpoena should cause a financial institution to review relevant account activity and transactions.[7]

---

4. A written request from a federal law enforcement agency should be issued by a supervisory agent or by an attorney within a United States Attorney's Office or another office of the Department of Justice. If a state or local law enforcement agency requests that an account be maintained, then the financial institution should obtain a written request from a supervisor of the state or local law enforcement agency or from an attorney within a state or local prosecutor's office. For additional guidance about the content of "keep open" requests, see "Requests by Law Enforcement for Financial Institutions to Maintain Accounts," available at https://www.fincen.gov/resources/statutes-regulations/guidance/requests-law-enforcement-financial-institutions-maintain.
5. *See* 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR Chapter X (FinCEN).
6. *See* https://www.fincen.gov/sites/default/files/shared/sar_tti_21.pdf at p. 53.
7. *See* https://www.fincen.gov/sites/default/files/shared/sar_tti_10.pdf at p. 43.

The financial institution should determine whether SAR filing is necessary based on its assessment of all information available and applicable regulatory requirements. If a financial institution files a SAR on a customer or transaction following the receipt of a grand jury subpoena or other law enforcement inquiry, the SAR should focus on the facts and circumstances that support a finding of suspicious activity rather than the subpoena or inquiry itself.[8]

Question 3: Maintaining a Customer Relationship Following the Filing of a SAR or Multiple SARs

Is a financial institution required to terminate a customer relationship following the filing of a SAR or multiple SARs?

No. There is no BSA regulatory requirement to terminate a customer relationship after the filing of a SAR or any number of SARs. The decision to maintain or close a customer relationship as a result of the identification of suspicious activity is a determination for a financial institution to make based on the information available to it, its assessment of money laundering or other illicit financial activity risks, and established policies, procedures, and processes.

Financial institutions have the flexibility to develop risk-based procedures and monitoring processes for the purpose of updating the customer risk profile and determining when to maintain or close accounts. Generally, financial institutions have policies, procedures, and processes in place that establish an escalation process for decisions to maintain or terminate customer relationships based on relevant factors, including SAR filing(s). These processes establish criteria, including when review by senior management and legal staff is warranted, for the decision to maintain or terminate the customer relationship in light of elevated risk factors. As indicated above, there is no specific number of SAR filings that a financial institution must consider to trigger any particular escalation step. Rather, the number of SAR filings and other factors that trigger escalation steps may vary based upon, among other things, the risk profile of the customer, including the geographical locations involved, the volume and type of transactions conducted by customers, the type of account, and the types of SARs filed by the financial institution in relation to the customer.[9]

Question 4: SAR Filing on Negative News Identified in Media Searches

Is a financial institution required to file a SAR based solely on negative news?

No. The existence of negative news related to a customer or other activity at a financial institution does not by itself indicate that the criteria requiring the filing of a SAR have been met, and does not automatically require the filing of a SAR by a financial institution. A financial institution may review media reports, news articles and/or other references to assist in its performance of customer due diligence, as well as its evaluation of any transactions or activity it

8. Financial institutions are reminded that grand jury proceedings and certain law enforcement inquiries may be subject to specific confidentiality provisions. For example, National Security Letters are subject to certain disclosure prohibitions. *See, e.g.*, https://www.fincen.gov/sites/default/files/shared/sar_tti_08.pdf at p. 36.

9. As referenced in Question 1, there may be instances where law enforcement requests a financial institution to maintain an account relationship, notwithstanding potential suspicious activity, and the financial institution should continue filing SARs, or continuing activity SARs, as applicable.

© gettechnical inc 2021

considers unusual or potentially suspicious. For example, negative news may cause a financial institution to review customer activity as well as other related information, such as that of third parties with transactions involving the customer's account. As with other identified unusual or potentially suspicious activity, financial institutions should comply with applicable regulatory requirements and follow their established policies, procedures, and processes to determine the extent to which it investigates and evaluates negative news, in conjunction with its review of transactions occurring by, at, or through the institution, to determine if a SAR filing is required.

Question 5: SAR Monitoring on Multiple Negative Media Alerts

If there are multiple negative news alerts based on the same event, is a financial institution expected to independently investigate each of those alerts?

No. In circumstances where there are multiple negative news alerts (as identified through monitoring for unusual or suspicious activity) based on the same underlying events, a financial institution does not need to independently investigate each alert, but rather may consider whether the alert contains new or different information that warrants further investigation or whether the negative news otherwise assists or informs the evaluation of the activity at issue. Many financial institutions maintain a process for managing a high volume of alerts generated by news. This type of process will allow the financial institution to identify and evaluate new information and assess whether to update customer information and risk profile, investigate transactions which may result in the filing of a SAR, or escalate or terminate a customer relationship, as appropriate consistent with its policies, procedures, and processes. Financial institutions have flexibility in developing risk-based procedures and monitoring processes for the purpose of complying with customer due diligence requirements and, where appropriate, consideration of negative news.[10]

Question 6: Information in Data Fields and Narrative

Do financial institutions need to repeat information in the SAR narrative that has already been included in other SAR data fields?

No. As stated in the SAR instructions, information provided in other sections of a SAR does not need to be repeated in the narrative unless necessary to provide a clear and complete description of the suspicious activity.[11] Consistent with FinCEN's SAR instructions, financial institutions should focus the SAR narrative on the information necessary to enable the reader to understand the activity reported, including what was unusual or irregular about the activity

10. Customer Due Diligence (CDD) regulations (31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210) do not categorically require the performance of media searches or particular screenings. However, in certain circumstances, a financial institution might assess, on the basis of risk, that a customer presents a higher risk profile and, accordingly, collect more information (such as media searches) to better understand the customer relationship. Such information also assists a financial institution in determining when transactions are potentially suspicious. *See, e.g.*, "Frequently Asked Questions Regarding Customer Due Diligence Requirements for Covered Financial Institutions," August 3, 2020, https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-regarding-customer-due-1.

11. *See* FinCEN Suspicious Activity Report Electronic Filing Requirements, last updated July 2020, available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf at p. 167.

© gettechnical inc 2021

that caused suspicion. For example, granular detail (such as subject identification data) that is reported in the appropriate SAR data fields does not need to be repeated in the SAR narrative, unless such information is necessary to clearly describe the activity reported. Additionally, the SAR narrative may benefit from information about the suspicious activity that may not be readily evident from SAR data fields alone, such as an explanation about why the filer selected different characterizations of suspicious activity in the SAR data fields. Note, however, that FinCEN Advisories may include requests for financial institutions to incorporate certain terms in SAR field 2 (Financial Institution Note to FinCEN) and in the narrative to indicate a connection between the suspicious activity being reported and the subject of an advisory.[12]

Question 7: SAR Character Limits

Should financial institutions file additional SARs on the same suspicious activity to accommodate narratives that are longer than the SAR narrative character limits?

No. Filers must provide a clear, complete, and concise description of the suspicious activity that led to the decision to file the SAR.[13] A financial institution that reaches the SAR narrative character limit should not file an additional SAR to continue a narrative in order to avoid duplicate filings on the same activity in the database.[14] Instead, filers should focus the relevant information in the narrative as much as possible, and may include additional, relevant information as an attachment to the SAR, or note that it is available as supporting documentation.

To keep narratives within the character limit and enable efficient review of information (such as transaction records) that is displayed most clearly in tabular format, filers can include a single comma-separated values (CSV) file with no more than one megabyte of data as an attachment to a SAR. If a filer wishes to include information in a tabular format in a SAR, the CSV attachment should be used; filers should not include tabular information within the SAR narrative.

Filers must retain all supporting documentation or a business record equivalent for five years from the date of the report.[15] All supporting documentation (such as copies of instruments; receipts; sale, transaction or clearing records; photographs; and surveillance audio or video recordings) must be made available to appropriate authorities upon request.[16]

12. For additional information on FinCEN Advisories, see https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets.
13. *See* FinCEN Suspicious Activity Report Electronic Filing Requirements, last updated July 2020, available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf at p. 167.
14. A SAR narrative can have a maximum of 20,000 characters. For more information, see FinCEN Suspicious Activity Report Electronic Filing Requirements, last updated July 2020, available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf at p. 105.
15. 31 CFR § 1010.430; 31 CFR § 1010.320; subpart C of the relevant financial institution part of 31 CFR Chapter X.
16. 31 CFR § 1010.320; subpart C of the relevant financial institution part of 31 CFR Chapter X.

© gettechnical inc 2021

DEPARTMENT OF FINANCIAL SERVICES: BANKING DIVISION TRANSACTION MONITORING AND FILTERING PROGRAM REQUIREMENTS AND CERTIFICATIONS

Department of Financial Services
Superintendent's Regulations

Part 504
BANKING DIVISION TRANSACTION MONITORING AND FILTERING PROGRAM REQUIREMENTS AND CERTIFICATIONS

(Statutory authority: Banking Law §§37(3)(4); Financial Services Law §302)

Sec.

§ 504.1 Background
§ 504.2 Definitions
§ 504.3 Transaction Monitoring and Filtering Program Requirements
§ 504.4 Annual Certifications
§ 504.5 Penalties/Enforcement Actions
§ 504.6 Effective Date

§ 504.1 Background.

The Department of Financial Services (the "Department") has been involved in investigations into compliance by Regulated Institutions, as defined below, with applicable Bank Secrecy Act/Anti-Money Laundering laws and regulations[1] ("BSA/AML") and Office of Foreign Assets Control of the Treasury Department ("OFAC")[2] requirements implementing federal economic and trade sanctions.[3]

As a result of these investigations, the Department identified shortcomings in the transaction monitoring and filtering programs of these institutions attributable to a lack of robust governance, oversight, and accountability at senior levels. Based on not only this experience, but also its regular examinations for safety and soundness, along with other factors, the Department has reason to believe that financial institutions have shortcomings in their transaction monitoring and filtering programs.

As a result, the Department has determined to clarify the required attributes of a Transaction Monitoring and Filtering Program and to require that the Board of Directors or Senior Officer(s), as applicable, of each Regulated Institution submit to the Superintendent annually a Board

[1] With respect to federal laws and regulations, *see* 31 U.S.C. § 5311, *et seq.* and 31 CFR Chapter X. For New York State regulations, *see* Part 115 (3 NYCRR 115), Part 116 (3 NYCRR 116), Part 416 (3 NYCRR 416) and Part 417 (3 NYCRR 417).
[2] 31 CFR part 501 *et seq*.
[3] For information regarding the Unites States Code, the Code of Federal Regulations and the Federal Register, see Supervisory Policy G-1.

© gettechnical inc 2021

Resolution or Compliance Finding, as defined in this Part, confirming the steps taken to ascertain compliance by the Regulated Institution with this Part.

This regulation implements these requirements.

§ 504.2 Definitions.

The following definitions apply in this Part:

(a) "Annual Board Resolution or Senior Officer Compliance Finding" means a board resolution or senior officer(s) finding in the form set forth in Attachment A.

(b) "Bank Regulated Institutions" means all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law (the "Banking Law") and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York.

(c) "Board of Directors" means the governing board of every Regulated Institution or the functional equivalent if the Regulated Institution does not have a Board of Directors.

(d) "Nonbank Regulated Institutions" shall mean all check cashers and money transmitters licensed pursuant to the Banking Law.

(e) "Regulated Institutions" means all Bank Regulated Institutions and all Nonbank Regulated Institutions.

(f) "Risk Assessment" means an on-going comprehensive risk assessment, including an enterprise wide BSA/AML risk assessment, that takes into account the institution's size, staffing, governance, businesses, services, products, operations, customers, counterparties, other relations and their locations, as well as the geographies and locations of its operations and business relations;

(g) "Senior Officer(s)" shall mean the senior individual or individuals responsible for the management, operations, compliance and/or risk of a Regulated Institution including a branch or agency of a foreign banking organization subject to this Part.

(h) "Suspicious Activity Reporting" means a report required pursuant to 31 U.S.C. § 5311 *et seq.* that identifies suspicious or potentially suspicious or illegal activities.

(i) "Transaction Monitoring Program" means a program that includes the attributes specified in Subdivisions (a), (c) and (d) of Section 504.3.

(j) "Filtering Program" means a program that includes the attributes specified in Subdivisions (b), (c) and (d) of Section 504.3.

© gettechnical inc 2021

(k) "Transaction Monitoring and Filtering Program" means a Transaction Monitoring Program, and a Filtering Program, collectively.

§ 504.3 Transaction Monitoring and Filtering Program Requirements.

(a) Each Regulated Institution shall maintain a Transaction Monitoring Program reasonably designed for the purpose of monitoring transactions after their execution for potential BSA/AML violations and Suspicious Activity Reporting, which system may be manual or automated, and which shall include the following attributes, to the extent they are applicable:

1. be based on the Risk Assessment of the institution;
2. be reviewed and periodically updated at risk-based intervals to take into account and reflect changes to applicable BSA/AML laws, regulations and regulatory warnings, as well as any other information determined by the institution to be relevant from the institution's related programs and initiatives;
3. appropriately match BSA/AML risks to the institution's businesses, products, services, and customers/counterparties;
4. BSA/AML detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities;
5. end-to-end, pre-and post-implementation testing of the Transaction Monitoring Program, including, as relevant, a review of governance, data mapping, transaction coding, detection scenario logic, model validation, data input and Program output;
6. documentation that articulates the institution's current detection scenarios and the underlying assumptions, parameters, and thresholds;
7. protocols setting forth how alerts generated by the Transaction Monitoring Program will be investigated, the process for deciding which alerts will result in a filing or other action, the operating areas and individuals responsible for making such a decision, and how the investigative and decision-making process will be documented; and
8. be subject to an on-going analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

(b) Each Regulated Institution shall maintain a Filtering Program, which may be manual or automated, reasonably designed for the purpose of interdicting transactions that are prohibited by OFAC, and which shall include the following attributes, to the extent applicable:

1. be based on the Risk Assessment of the institution;

© gettechnical inc 2021

2. be based on technology, processes or tools for matching names and accounts[4], in each case based on the institution's particular risks, transaction and product profiles;

3. end-to-end, pre- and post-implementation testing of the Filtering Program, including, as relevant, a review of data matching, an evaluation of whether the OFAC sanctions list and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and Program output;

4. be subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the OFAC sanctions list and the threshold settings to see if they continue to map to the risks of the institution; and

5. documentation that articulates the intent and design of the Filtering Program tools, processes or technology.

(c) Each Transaction Monitoring and Filtering Program shall require the following, to the extent applicable:

1. identification of all data sources that contain relevant data;

2. validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Program;

3. data extraction and loading processes to ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems, if automated systems are used;

4. governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited;

5. vendor selection process if a third party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it;

6. funding to design, implement and maintain a Transaction Monitoring and Filtering Program that complies with the requirements of this Part;

7. qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filings; and

---

[4] The technology used in this area may be based on automated tools that develop matching algorithms, such as those that use various forms of so-called "fuzzy logic" and culture-based name conventions to match names. This regulation does not mandate the use of any particular technology, only that the system or technology used must be reasonably designed to identify prohibited transactions.

© gettechnical inc 2021

8. periodic training of all stakeholders with respect to the Transaction Monitoring and Filtering Program.

(d) To the extent a Regulated Institution has identified areas, systems, or processes that require material improvement, updating or redesign, the Regulated Institution shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Superintendent.

§ 504.4 Annual Board Resolution or Senior Officer(s) Compliance Finding.

To ensure compliance with the requirements of this Part, each Regulated Institution shall adopt and submit to the Superintendent a Board Resolution or Senior Officer(s) Compliance Finding in the form set forth in Attachment A by April 15th of each year. Each Regulated Institution shall maintain for examination by the Department all records, schedules and data supporting adoption of the Board Resolution or Senior Officer(s) Compliance Finding for a period of five years.

§ 504.5 Penalties/Enforcement Actions.

This regulation will be enforced pursuant to, and is not intended to limit, the Superintendent's authority under any applicable laws.

§ 504.6 Effective Date.

This Part shall be effective January 1, 2017. Regulated Institutions will be required to prepare and submit to the Superintendent Annual Board Resolutions or Senior Officer(s) Compliance Findings under § 504.4 commencing April 15, 2018.

© gettechnical inc 2021

ATTACHMENT A

_____

(Regulated Institution Name)

APRIL 15, 20____

Annual Board Resolution or Senior Officer(s) Compliance Finding For Bank Secrecy Act/Anti-Money Laundering and Office of Foreign Asset Control Transaction Monitoring and Filtering Program

Whereas, in compliance with the requirements of the New York State Department of Financial Services (the "Department") that each Regulated Institution maintain Transaction Monitoring and Filtering Program in compliance with Section 504.3; and

Whereas, Section 504.4 requires that the Board of Directors or a Senior Officer(s), as appropriate, adopt and submit to the Superintendent a Board Resolution or Senior Officer Compliance Finding confirming its or such individual's findings that the Regulated Institution is in compliance with Section 504.3 of this Part 504;

NOW, THEREFORE, the Board of Directors or Senior Officer certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary to adopt this Board Resolution or Senior Officer Compliance Finding;

(2) The Board of Directors or Senior Officer(s) has taken all steps necessary to confirm that (name of Regulated Institution) has a Transaction Monitoring and Filtering Program that complies with the provisions of Section 504.3; and

(3) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Transaction Monitoring and the Filtering Program of (name of Regulated Institution) as of _____ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended _____ (year for which Board Resolution or Compliance Finding is provided) complies with Section 504.3.

© gettechnical inc 2021

Signed by each member of the Board of Directors or Senior Officer(s)

(Name)_____ Date:

© gettechnical inc 2021

Board of Governors of the Federal Reserve System
Commodity Futures Trading Commission
Consumer Financial Protection Bureau
Federal Deposit Insurance Corporation
Federal Trade Commission
National Credit Union Administration
Office of the Comptroller of the Currency
Securities and Exchange Commission

Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults

PURPOSE

The Board of Governors of the Federal Reserve System (Federal Reserve), Commodity Futures Trading Commission (CFTC),[1] Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), Federal Trade Commission (FTC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Securities and Exchange Commission (SEC) are issuing this guidance to financial institutions to clarify the applicability of privacy provisions of the Gramm-Leach-Bliley Act (GLBA) to reporting suspected financial exploitation of older adults.

Employees of depository institutions and other financial service providers that constitute "financial institutions" for purposes of the GLBA may observe signs of possible financial exploitation of an older adult. Various federal and state authorities either require or encourage reporting of this type of information to the appropriate agency. This guidance clarifies that reporting suspected financial abuse of older adults to appropriate local, state, or federal agencies does not, in general, violate the privacy provisions of the GLBA or its implementing regulations.[2] In fact, specific privacy provisions of the GLBA and its

[1] The CFTC is issuing this document as staff guidance.

[2] While this guidance discusses when reporting is allowed under the GLBA, it does not address any other federal or state laws that may regulate such reporting. Also, the guidance does not specifically address risk management expectations for financial institutions related to the reporting of elder abuse.

© gettechnical inc 2021

implementing regulations permit the sharing of this type of information under appropriate circumstances without complying with notice and opt-out requirements.[3]

BACKGROUND

Elder abuse includes the illegal or improper use of an older adult's funds, property, or assets.[4] Recent studies suggest that financial exploitation is the most common form of elder abuse and that only a small fraction of incidents are reported.[5] Older adults can become targets of financial exploitation by family members, caregivers, scam artists, financial advisers, home repair contractors, fiduciaries (such as agents under power of attorney and guardians), and others. Older adults are attractive targets because they may have significant assets or equity in their homes. They may be especially vulnerable due to isolation, cognitive decline, physical disability, health problems, and/or the recent loss of a partner, family member, or friend. Financial institutions can play a key role in preventing and detecting elder financial exploitation. A financial institution's familiarity with older adults it encounters may enable it to spot irregular transactions, account activity, or behavior.[6] Prompt reporting of suspected financial exploitation to adult protective services, law enforcement,[7] and/or long-term care ombudsmen can trigger appropriate intervention, prevention of financial losses, and other remedies.

DISCUSSION OF PRIVACY PROTECTIONS

---

[3] This guidance's analysis of the GLBA's privacy provisions builds on joint guidance issued by several federal agencies in 2002 that specifically addressed disclosures to the Michigan Family Independence Agency. *See* Letter to Hon. Debbie Stabenow, July 3, 2002, *available at* http://www.americanbar.org/content/dam/aba/administrative/law_aging/2011/2011_aging_ea_bank_rptg_op_ltr.authcheckdam.pdf.

[4] *See* the National Center on Elder Abuse definitions *available at* http://www.ncea.aoa.gov/FAQ/Type_Abuse/index.aspx. The Older Americans Act, as amended by the Elder Justice Act of 2009, defines exploitation as "the fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual, including a caregiver or fiduciary, that uses the resources of an elder for monetary or personal benefit, profit, or gain, or that results in depriving an elder of rightful access to, or use of, benefits, resources, belongings, or assets." 42 U.S.C. 1397j(8).

[5] Acierno, R., M. A. Hernandez, A. B. Amstadter, H. S. Resnick, K. Steve, W. Muzzy, and D. G. Kilpatrick, "Prevalence and Correlates of Emotional, Physical, Sexual and Financial Abuse and Potential Neglect in the United States: The National Elder Mistreatment Study," *American Journal of Public Health* 100(2): 292–97; Lifespan of Greater Rochester, Inc., et al., *Under the Radar: New York State Elder Abuse Prevention Study,* (Rochester, NY: Lifespan of Greater Rochester, Inc., May 2011).

[6] Treasury Department rules require recipients of federal nontax payments to receive payment by electronic funds transfer, with an allowance for certain waivers from the requirement. The rule applies to recipients of Social Security, Veterans Affairs, Supplemental Security Income, Railroad Retirement Board, Department of Labor, and Office of Personnel Management benefit payments. Benefit recipients may have payments directly deposited to an account at a financial institution or to a *Direct Express* debit card account. *See* 75 Fed. Reg. 80315 (Dec. 22, 2010). Financial institutions should be mindful that this change may result in additional electronic funds transfer activity involving the accounts of older adults.

[7] Financial institutions file "Suspicious Activity Reports" with the Financial Crimes Enforcement Network (FinCEN), a Bureau of the U.S. Department of the Treasury, involving money laundering and terrorist financing as well as activities related to elder abuse and other consumer fraud. The reports assist law enforcement in identifying individuals and organizations involved in financial crime. *See* FinCEN, Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation, FIN-2011-A003 (Feb. 22, 2011), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf.

© gettechnical inc 2021

The GLBA establishes a general rule that a financial institution may not disclose any nonpublic personal information about a consumer to any nonaffiliated third party unless the financial institution first provides the consumer with a notice that describes the disclosure (as well as other aspects of its privacy policies and practices) and a reasonable opportunity to opt out of the disclosure, and the consumer does not opt out. However, section 502(e) of the GLBA provides a variety of exceptions to this general rule that permit a financial institution to disclose information to nonaffiliated third parties without first complying with notice and opt-out requirements. Generally, disclosure of nonpublic personal information about consumers to local, state, or federal agencies for the purpose of reporting suspected financial abuse of older adults will fall within one or more of the exceptions.[8] These disclosures of information may be made either at the agency's request or on the financial institution's initiative.

The following are specific exceptions to the GLBA's notice and opt-out requirement that, to the extent applicable, would permit sharing of nonpublic personal information about consumers with local, state, or federal agencies for the purpose of reporting suspected financial abuse of older adults without the consumer's authorization and without violating the GLBA:

- A financial institution may disclose nonpublic personal information to comply with federal, state, or local laws, rules and other applicable legal requirements, such as state laws that require reporting by financial institutions of suspected abuse. (15 U.S.C. 6802(e)(8) and implementing regulations at ____.15(a)(7)(i)).[9]
- A financial institution may disclose nonpublic personal information to respond to a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by federal, state, or local authorities or to respond to judicial process or government regulatory authorities having jurisdiction for examination, compliance, or other purposes as authorized by law. (15 U.S.C. 6802(e)(8) and implementing regulations at ____.15(a)(7)(ii)-(iii)).
- A financial institution may disclose nonpublic personal information to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability. (15 6802(e)(3)(B) and implementing regulations at ____.15(a)(2)(ii)). For example, this exception generally would allow a financial institution to disclose to appropriate authorities nonpublic personal information in order to:
  - report incidents that result in taking an older adult's funds without actual consent, or
  - report incidents of obtaining an older adult's consent to sign over assets through misrepresentation of the intent of the transaction.
- To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*), a financial institution may disclose nonpublic personal information to law enforcement agencies (including the CFPB, the federal functional regulators, and the FTC), self-regulatory organizations, or for an investigation on a matter related to public safety. (15 U.S.C. 6802(e)(5) and implementing regulations at ____.15(a)(4)).

[8] *See* Section 502(e) of the GLBA (15 U.S.C. 6802(e)).

[9] The CFPB's, FTC's, CFTC's, and SEC's implementing regulations are contained in 12 CFR part 1016, 16 CFR part 313, 17 CFR part 160, and 17 CFR part 248, respectively. For ease of reference, this discussion uses the shared numerical suffix of each of these agencies' regulations.

© gettechnical inc 2021

In addition, a financial institution may disclose nonpublic personal information with the consumer's consent or consent of the consumer's legal representative. (15 U.S.C. 6802(e)(2) and implementing regulations at ____.15(a)(1)).

POSSIBLE SIGNS OF FINANCIAL ABUSE OF OLDER ADULTS

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published an advisory in February 2011 that describes potential signs of elder financial exploitation that might trigger the filing of a Suspicious Activity Report (SAR).[10] As described in the advisory, among the possible signs of abuse are:

- Erratic or unusual banking transactions, or changes in banking patterns:
    - Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;
    - Sudden non-sufficient fund activity;
    - Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;
    - Debit transactions that are inconsistent for the older adult;
    - Uncharacteristic attempts to wire large sums of money; or
    - Closing of CDs or accounts without regard to penalties.

- Interactions with older adults or caregivers:[11]
    - A caregiver or other individual shows excessive interest in the older adult's finances or assets, does not allow the older adult to speak for himself, or is reluctant to leave the older adult's side during conversations;
    - The older adult shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;
    - The financial institution is unable to speak directly with the older adult, despite repeated attempts to contact him or her;
    - A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the older adult without proper documentation;
    - The older adult moves away from existing relationships and toward new associations with other "friends" or strangers;
    - The older adult's financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual; or
    - The older adult lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

[10] *See* footnote 6 above.
[11] References to "caregiver" or "caretaker" also may apply to other individuals who may be involved in transactions of the type described in the FinCEN advisory.

© gettechnical inc 2021

Further information about the use of Suspicious Activity Reports to report suspected elder financial exploitation is available in FinCEN's "The SAR Activity Review" published in May

2013.[12] In addition, if financial institutions or other organizations are interested in raising public awareness among older adults and their caregivers about preventing, identifying, and responding to elder financial exploitation, *Money Smart for Older Adults*, a financial resource tool, serves as a helpful source of training and information.[13]

[12] *See* "The SAR Activity Review: Trends Tips & Issues," Issue 23, May 2013, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf.

[13] *Money Smart for Older Adults* (June 2013), *available at* www.fdic.gov or www.consumerfinance.gov.

© gettechnical inc 2021

CFPB BLOG: BANKS CAN HELP SPOT ELDER FINANCIAL EXPLOITATION AND ABUSE (9/24/13)

An older Oklahoma resident began receiving sweepstakes offers in the mail after her 90-year-old husband moved into a nursing home. Just send $50, $100, $2000, even $5000 to claim your prize, they promised. When she asked a bank employee to help her send a large amount of cash in the mail, the bank investigated. It turned out the older customer had been writing as many as 90 checks a month to collect promised prizes that never materialized. The bank contacted the Postal Inspection Service to investigate and the authorities intervened.

A 98-year-old lawyer was scammed by a purported friend who loaned him office space and then accessed financial records stored there. When the older man was hospitalized for hip surgery, the 76-year-old friend drained $330,000 from bank accounts and used the money to pay for a trip to Puerto Rico and purchases at a variety of stores. Ultimately, the victim's banks alerted authorities because of concerns about unusual activity on the accounts.

As we travel the country, we hear more stories of banks, credit unions, money transmitters, and other financial services providers spotting financial abuse targeted at older adults. Some of these are success stories like the ones we just shared: the financial institution makes a timely report, and authorities can prevent the theft, prosecute the perpetrator and help the victim.

But sometimes financial institution personnel are confused. They want to help protect the consumer, but are unsure whether privacy laws allow them to share a consumer's personal information with law enforcement and other authorities that can take action.

That's why today, along with seven other federal agencies, we released guidance on this issue for financial institutions. The guidance clarifies for banks and other financial services providers that reporting suspected elder financial exploitation to appropriate authorities does not generally violate the privacy provisions of the Gramm-Leach-Bliley Act, a federal law.

Reporting elder abuse is the right thing to do

Financial institutions often spot the red flags for abuse sooner than anyone else. We can only stop the financial exploitation of older adults through coordinated efforts at the community, state and national levels. Please join us in working to prevent, detect, and respond to this national problem and help prevent a disaster from happening to vulnerable elders across the country and in your community.

© gettechnical inc 2021

FINCEN: 2012 SAR DATA REVEALS DROP IN MORTGAGE FRAUD (8/20/13)

FOR IMMEDIATE RELEASE
August 20, 2013

MEDIA CONTACT: Steve Hudak
703-905-3770

FinCEN 2012 SAR Data Reveals Drop in Suspected Mortgage Fraud

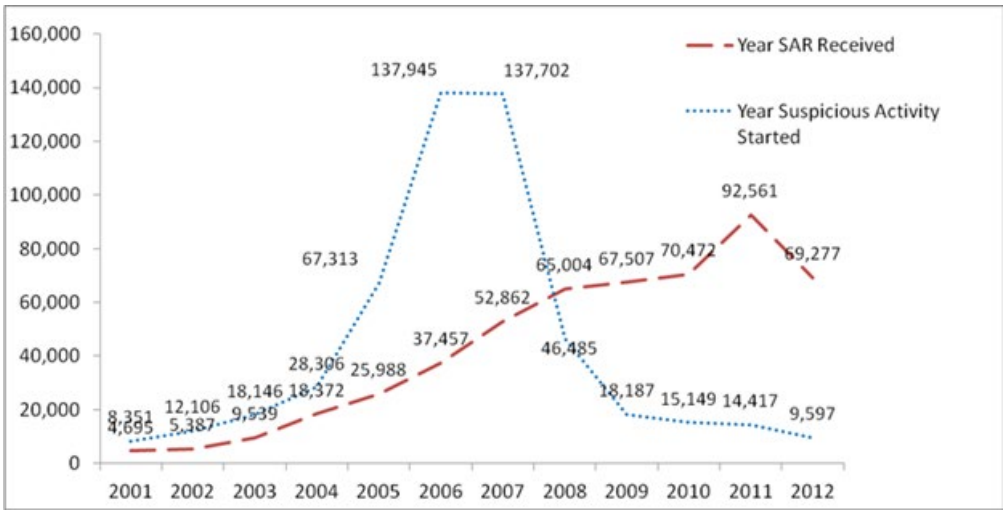
Data Confirms Spike in 2006, 2007 Suspicious Activity

VIENNA, Va. – The Financial Crimes Enforcement Network (FinCEN) today released an analysis of Mortgage Fraud SAR Filings in Calendar Year 2012. FinCEN's data on suspected mortgage fraud shows that reports declined 25 percent in 2012 (from 92,561 to 69,277) as compared to the previous year. The past three years of suspected mortgage fraud suspicious activity reports (SARs), if counted by the date they were received by FinCEN, accounted for approximately 46 percent of the past decade's mortgage fraud SARs. However, suspicious activity is often only recognized and reported years after loan origination, after a review of origination documents is prompted by a loan default, repurchase demand, or other factors. As a result, many mortgage fraud SARs are filed much later than the date that the suspicious activity actually began. Thus in 2012, 57 percent of SARs received reported mortgage loan fraud (MLF) activities that started more than 5 years before the SAR was filed.

The bulk of FinCEN's MLF SARs, regardless of filing date, reference suspicious activity that filers believe began in calendar years 2006 and 2007. The following chart depicts the number of annual mortgage fraud SAR filings based on the year FinCEN received the SAR, versus the year that the SAR filer believed the suspicious activity actually began (which was usually at loan origination). It shows that there was an extraordinary concentration of suspicious mortgage origination activity beginning in 2006 and 2007, the years immediately preceding the financial crisis of 2008.

© gettechnical inc 2021

Number of Mortgage Fraud SARs by Activity Start Date and Year Received



Depository institutions filed 37,457 MLF SARs in 2006 and 52,862 in 2007. At the time, those numbers represented huge increases over previous years, but they seriously underrepresented the amount of suspicious mortgage fraud activity that could have potentially been reported in those years if the suspicious activity had been detected closer to loan origination.

###

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

© gettechnical inc 2021

FINCEN: SUSPICIOUS ACTIVITY RELATED TO MORTGAGE LOAN FRAUD (8/16/12)

Advisory

FIN-2012-A009
Issued: August 16, 2012
Subject: Suspicious Activity Related to Mortgage Loan Fraud

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to highlight activity related to mortgage loan fraud so that financial institutions may better assist law enforcement when filing Suspicious Activity Reports (SARs). This Advisory, which consolidates certain information from previously issued FinCEN reports, contains examples of common fraud schemes and potential "red flags" for activity related to mortgage loan fraud. Using this additional information, the vigilance of financial institutions, together with law enforcement efforts against illicit mortgage-related activities, will help protect financial institutions and their customers from financial loss, and support the housing markets and the U.S. financial system as a whole.

This Advisory supports the efforts of the Financial Fraud Enforcement Task Force (FFETF),[40] the U.S. Department of the Treasury's broader initiatives to ensure that U.S. financial institutions are not used as conduits for illicit activity, and a FinCEN and U.S. Department of Housing and Urban Development (HUD) OIG mortgage fraud initiative.

Types of Mortgage Loan Fraud Identified by Law Enforcement

The following list identifies types of mortgage loan fraud, which are primarily based upon schemes and scams frequently reported or described in SARs or identified by our law enforcement and regulatory partners. This information is intended to assist financial institutions in identifying when illicit activities occur in connection with mortgage loan transactions.

Occupancy fraud: Occurs when borrowers, to obtain favorable loan terms, claim that subject properties will be their primary residences instead of vacation homes or investment properties. It also occurs when subjects apply for loans for properties that others, such as family members, will actually occupy.

Income fraud: Includes both overstating income to qualify for larger mortgages and understating income to qualify for hardship concessions and modifications.

[40] For more information on the FFETF and its current initiatives, please visit http://www.fincen.gov/fraudenftaskforce.html..

© gettechnical inc 2021

Appraisal fraud: Includes both overstating home value to obtain more money from a sale of property or cash-out refinancing, and understating home value in connection with a plan to purchase a property at a discount to market value.

Employment fraud: Includes misrepresenting whether, where, and for how long borrowers have been employed; whether borrowers are unemployed or collecting unemployment benefits; and whether borrowers are independent contractors or business owners.

Liability fraud: Occurs when borrowers fail to list significant financial liabilities, such as other mortgages, car loans, or student loans, on mortgage loan applications. Without complete liability information, lenders cannot accurately assess borrowers' ability to repay debts.

Debt elimination schemes:[41] Involves the use of fake legal documents and alternative payment methods to argue that existing mortgage obligations are invalid or illegal, or to purport to extinguish mortgage balances. Individuals orchestrating debt elimination schemes typically charge borrowers a fee for these debt elimination "services."

Foreclosure rescue scams:[42] Targets financially distressed homeowners with fraudulent offers of services or advice aimed at stopping or delaying the foreclosure process. Some of these scams require homeowners to transfer title - or make monthly mortgage payments - to the purported "rescuer," rather than the real holder of the mortgage. Some foreclosure rescue scams require homeowners to pay fees before receiving "services," and are known as "advance fee" schemes.

Social Security Number (SSN) Fraud and other Identify Theft:[43] Includes the use of an SSN or other government identification card or number that belongs to someone other than the applicant in a loan application. Identity Theft includes broader use of another's identity or identifiers (beyond an SSN) to obtain a mortgage or perpetrate a "fraud for profit" scheme.

Home Equity Conversion Mortgage (HECM):[44] Financial institutions need be aware of illegal "reverse mortgage" schemes, which targets seniors who own a home or who are coerced into taking title to a home, for the purpose of stealing or otherwise acquiring some or all of the funds the senior receives from a government HECM program. HECM fraud may involve other frauds, including appraisal fraud (to increase the stated value of the home), investment fraud to acquire the HECM funds from the senior under the guise of

[41] For additional information pertaining to schemes of this type, please see the June 2010 Advisory, available at: http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-a006.pdf.
[42] For additional information pertaining to foreclosure rescue fraud schemes, please see the April 2009 Advisory, available at: http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-a001.pdf.
[43] For additional information and resources from FinCEN and links to other governmental efforts to combat identity theft, please visit FinCEN's website at: http://www.fincen.gov/help4victims.html.
[44] For additional information pertaining to Home Equity Conversion Mortgage (HECM) fraud schemes, please see the April 2010 Advisory, available at: http://www.fincen.gov/statutes_regs/guidance/html/fin-2010-a005.html.

© gettechnical inc 2021

future profits for the senior, and identify theft to acquire HECM funds without the knowledge of the senior who owns the property.

Possible Red Flag Indicators of Mortgage Loan Fraud

The following highlights potential red flag indicators of illicit activity related to mortgage fraud. These only indicate possible signs of fraudulent activity; they do not constitute an exhaustive list of common fraud schemes. No single red flag will be definitive proof of such activity and many apply to multiple fraud schemes. Instead, it is important to view any red flag(s) in the context of other indicators and facts, such as the specific role of the financial institution within mortgage loan-related transaction(s), as well as the institution's knowledge of any associated fraud schemes. The presence of any of these red flags in a given transaction or business arrangement may indicate a need for further due diligence and a decision whether to file a SAR.

- Borrower/buyer submits invalid documents in order to cancel his or her mortgage obligations or to pay off his or her loan balance(s).
- Same notary public and/or other "authorized representative" preparing, signing, and sending packages of nearly identical debt elimination documents for multiple borrowers with outstanding mortgage balances.
- Same notary public and/or other "authorized representative" working with and/or receiving payments from unusually large numbers of borrowers.
- Falsification of certified checks, cashier's checks or "non-cash item checks" drawn against a borrower/buyer's account, rather than from the account of a financial institution.
- Borrower/buyer applies for a loan for a "primary residence " but does not reside in the new primary residence as indicated on the loan application; other individuals occupy the borrower/buyer's new primary residence indicating the property is being used as a secondary residence or income-generating property.
- Borrower/buyer of a younger age purchases his or her "primary residence" in a senior citizen residential development.
- Borrower/buyer requests refinancing for "primary residence" when public and personal documents indicate that the borrower/buyer resides somewhere other than the address on the loan application.
- Language included in a short sale contract indicates the property could be resold promptly. This possibly illegal "flipping" may occur regardless of whether the Federal Housing Administration (FHA) has re-enacted or waived its arms-length resale regulations to FHA buyers.
- Low appraisal values, non-arms length relationships between short sale buyers and sellers, or previous fraudulent sale attempts in short-sale transactions,.
- Agent of the buyer and/or seller in mortgage transaction is unlicensed.
- Past misrepresentations made by borrower/buyer in attempts to secure funding, property, refinance, and/or shorts sales.
- Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information.
- Apparent resubmission of rejected loan application with key borrower/buyer details changed or modified from individual borrower to company/corporation. This

activity may identify the same person attempting to secure a loan fraudulently through a straw-borrower or non-existent person.

- Borrower/buyer attempts to structure currency deposits/withdrawals, or otherwise to hide or disguise the true value of assets, in order to qualify for loan modification programs intended for those homeowners in financial distress.
- Request from third party affiliates on behalf of distressed homeowners to pay fees in advance of the homeowner receiving mortgage counseling, foreclosure avoidance, a loan modification, or other related services.
- Third party solicitation of distressed homeowners for purported mortgage counseling, foreclosure avoidance, loan modification, or other related services. These third parties may also claim to be associated with legitimate mortgage lenders, the U.S. government, or a U.S. government program.[45]

Suspicious Activity Reporting

If a financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity or an attempt to disguise funds derived from illegal activity, is designed to evade regulations promulgated under the Bank Secrecy Act, or lacks a business or apparent lawful purpose, the financial institution may be required to file a SAR.[46] When completing SARs on suspected mortgage loan fraud, financial institutions should indicate the type of mortgage loan fraud by entering the appropriate code in the FinCEN SAR and provide a detailed description in the SAR narrative. For activity that does not have a corresponding code, financial institutions should identify "Other" and describe the activity in the narrative.[47]

Financial institutions, when filing a SAR, are also requested, where available, to include in the narrative portion, the Conference of State Bank Supervisors' (CSBS) National Mortgage Licensing System and Registry (NMLS) assigned "NMLS Unique Identifier." As required by Section 1503 of the Secure and Fair Enforcement for Mortgage Licensing Act of 2008 (SAFE Act), a NMLS unique identifier is permanently assigned to each state-licensed or federally registered mortgage loan originator (MLO), as well as each company, branch, and control person that maintains a single account in NMLS. The value of the NMLS Unique Identifier has been recognized by the Federal Housing Finance Agency (FHFA) and HUD. Both federal agencies require that any loan purchased or securitized by Fannie Mae and Freddie Mac, or submitted for insurance by the FHA, must include the NMLS Unique Identifier for the company and individual MLO that originated the mortgage loan.

Questions or comments regarding the contents of this advisory or the June 2010 Advisory should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this

[45] For additional information pertaining to schemes of this type, please see the June 2010 Advisory, available at: http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-a006.pdf.
[46] See, e.g., 31 CFR § 1020.320 and 31 CFR § 1029.320
[47] For additional assistance on key terms related to types of real estate fraud, please see the Suspicious Activity Report (SAR) Advisory Key Terms Guidance, available at: http://www.fincen.gov/news_room/advisory/AdvisoryKeyTerms.html

© gettechnical inc 2021

information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

© gettechnical inc 2021

FINCEN BSA FAQ

https://www.fincen.gov/answers-frequently-asked-bank-secrecy-act-bsa-questions

Question 1: Is a depository institution required to file a Designation of Exempt Person form (FinCEN 110) in order to exempt transactions with a Federal Reserve Bank?

Answer 1: Depository institutions are not required to file a Designation of Exempt Person form (FinCEN 110) with respect to the transfer of currency to or from any of the 12 Federal Reserve Banks in accordance with an Interim Rule published by FinCEN in the Federal Register (65 FR 46356-46361) on July 28, 2000. This Interim Rule, which amends the CTR exemption regulation at 31 CFR 1020.315, became effective on July 31, 2000. (12/2017).

Question 2(a): Where can a depository institution obtain a copy of the Designation of Exempt Person form (FinCEN 110) which must be used to designate an eligible customer as an exempt person from currency transaction reporting rules of the Department of the Treasury (31 CFR 1020.315(c)).

Answer 2(a): The Designation of Exempt Person form is available from FinCEN's web site at https://www.fincen.gov/resources/filing-information (12/2017).

Question 2(b): Where does a depository institution file the Designation of Exempt Person form?

Answer 2(b): The Designation of Exempt Person form is filed with FinCEN though the BSA E-Filing system at https://bsaefiling.fincen.treas.gov/main.html. (12/2017)

Question 2(c): Does FinCEN provide depository institutions with a confirmation of receipt of the Designation of Exempt Person form (FinCEN 110)?

Answer 2(c): Designation of Exempt Person form (FinCEN 110) is filed electronically with FinCEN through the BSA E-Filing system. The filing institution is provided an acknowledgement that the report has been received. (12/2017)

Question 3: There are frequently asked questions regarding Repeated SAR Filings on the same Activity. The following discussion is contained in Section 5 of The SAR Activity Review – Trends, Tips & Issues (October 2000).

Answer 3: One of the purposes of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This is accomplished by the filing of a SAR that identifies the activity of concern. Should this activity continue over a period of time, it is useful for such information to be made

© gettechnical inc 2021

known to law enforcement (and the bank supervisors). As a general rule of thumb, organizations should report continuing suspicious activity with a report being filed at least every 90 days. This will serve the purposes of notifying law enforcement of the continuing nature of the activity, as well as provide a reminder to the organization that it must continue to review the suspicious activity to determine if other actions may be appropriate, such as terminating its relationship with the customer or employee that is the subject of the filing. (12/2000)

Question 4: There are frequently asked questions regarding Filing SARs on Continuing Activity after Law Enforcement Contact. The following discussion is contained in Section 6 of The SAR Activity Review – Trends, Tips & Issues (June 2001).

Answer 4: In some instances, after the filing of one or more SARs, law enforcement has contacted a financial institution requesting more specific information with regard to the suspect activity or requesting identified supporting documentation. In other instances, a law enforcement agency has contacted a financial institution to report that it does not intend to investigate the matter reported on the SAR.

If conduct continues for which a SAR has been filed, the guidance set forth in the October 2000 SAR Activity Review (Section 5 – Repeated SAR Filings on the Same Activity) should be followed (i.e., organizations should report continuing suspicious activity with a SAR being filed at least every 90 days) even if a law enforcement agency has declined to investigate or there is knowledge that an investigation has begun. The filing of SARs on continuing suspicious activity provides useful information to law enforcement and supervisory authorities. Moreover, the information contained in a SAR that one law enforcement agency has declined to investigate may be of interest to other law enforcement agencies, as well as supervisory agencies. (6/2001)

Question 5: There are frequently asked questions regarding Filing SARs on Activity Outside the United States. The following discussion is contained in Section 6 of The SAR Activity Review – Trends, Tips & Issues (June 2001).

Answer 5: Consistent with the SAR regulations, it is expected that financial institutions will file SARs on activity deemed to be suspicious even when a portion of the activity occurs outside of the United States or the funds involved in the activity originated from outside the United States. Although foreign-located operations of U.S. organizations are not required to file SARs, an organization may wish, for example, to file a SAR with regard to suspicious activity that occurs outside the United States that is so egregious that it has the potential to cause harm to the entire organization. (It is, of course, expected that foreign-located operations of U.S. organizations that identify suspicious activity will report such activity consistent with local reporting requirements in the foreign jurisdiction where the operation is located.) (6/2001)

Question 6: There are frequently asked questions regarding Cessation of Relationship/Closure of Account as a result of the identification of suspicious activity. The following discussion is contained in Section 5 of The SAR Activity Review – Trends, Tips & Issues (October 2000).

© gettechnical inc 2021

Answer 6: The closure of a customer account as the result of the identification of suspicious activity is a determination for an organization to make in light of the information available to the organization. A filing of a SAR, on its own, should not be the basis for terminating a customer relationship. Rather, a determination should be made with the knowledge of the facts and circumstances giving rise to the SAR filing, as well as other available information that could tend to impact on such a decision. It may be advisable to include the organization's counsel, as well as other senior staff, in such determinations. (12/2000)

Question 7: There are frequently asked questions regarding Timing for SAR Filings. The following discussion is contained in Section 5 of The SAR Activity Review – Trends, Tips & Issues (October 2000).

Answer 7: The SAR rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of the suspicious activity, unless no suspect can be identified, in which case, the time period for filing a SAR is extended to 60 days.

It may be appropriate for organizations to conduct a review of the activity to determine whether a need exists to file a SAR. The fact that a review of customer activity or transactions is determined to be necessary is not necessarily indicative of the need to file a SAR, even if a reasonable review of the activity or transactions might take an extended period of time. The time to file a SAR starts when the organization, in the course of its review or on account of other factors, reaches the position in which it knows, or has reason to suspect, that the activity or transactions under review meets one or more of the definitions of suspicious activity.

Of course, an expeditious review, wherever possible, is recommended and can be of significant assistance to law enforcement. In situations involving violations of law requiring immediate attention, the organization should immediately notify appropriate law enforcement and supervisory authorities, in addition to filing a SAR. (12/2000)

Question 8: There are frequently asked questions regarding the Disclosure of SARs and Underlying Suspicious Activity. The following discussion is contained in Section 5 of The SAR Activity Review – Trends, Tips & Issues (October 2000).

Answer 8: Federal law (31 U.S.C. 5318(g)(2)) prohibits the notification of any person that is involved in the activity being reported on a SAR that the activity has been reported. This prohibition effectively precludes the disclosure of a SAR or the fact that a SAR has been filed. However, this prohibition does not preclude, under Federal law, a disclosure in an appropriate manner of the facts that are the basis of the SAR, so long as the disclosure is not made in a way that indicates or implies that a SAR has been filed or that the information is included on a filed SAR.

The prohibition against disclosure can raise special issues when SAR records are sought by subpoena or court order. The SAR regulations direct organizations facing those issues to contact their primary supervisor, as well as FinCEN, to obtain guidance and direction on how to proceed. In several matters to date, government agencies have intervened to ensure

© gettechnical inc 2021

that the protection for filing organizations and the integrity of the data contained within the SAR database remain intact. (12/2000)

Question 9: There are frequently asked questions regarding the Prohibition on Notification. The following discussion is contained in Section 6 of The SAR Activity Review – Trends, Tips & Issues (June 2001).

Answer 9: As set forth in the October 2000 SAR Activity Review (Section 5 – Disclosure of SARs and Underlying Suspicious Activity), Federal law (31 U.S.C. 5318(g)(2)) prohibits the notification to any person that is involved in the activity being reported on a SAR that the activity has been reported. This prohibition extends to disclosures that could indirectly result in the notification to the subject of a SAR that a SAR has been filed, effectively precluding the disclosure of a SAR or even its existence to any persons other than appropriate law enforcement and supervisory agency or agencies. This prohibition does not preclude, under Federal law, a disclosure in an appropriate manner of the facts that are the basis of the SAR, so long as the disclosure is not made in a way that indicates or implies that a SAR has been filed or that information is included on a filed SAR.

In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised.

The prohibition on notification of a SAR filing can raise special issues when SAR filings are sought by subpoena or court order. The SAR regulations direct organizations facing these issues to contact their primary supervisor, as well as FinCEN, to obtain guidance and direction on how to proceed. In several matters to date, government agencies have intervened to ensure that the protection for filing organizations and the integrity of the data contained within the SAR database remain intact. (6/2001)

Question 10: There are frequently asked questions regarding Disclosure of SAR Documentation. The following discussion is contained in Section 6 of The SAR Activity Review – Trends, Tips & Issues (June 2001).

Answer 10: Under the SAR regulations, institutions filing SARs should identify within the SAR, and are directed to maintain all "supporting documentation" related to the activity being reported. Disclosure of supporting documentation related to the activity that is being reported on a SAR does not require a subpoena, court order, or other judicial or administrative process. Under the SAR regulations, financial institutions are required to disclose supporting documentation to appropriate law enforcement agencies, or FinCEN, upon request. (6/2001)

Question 11: There are frequently asked questions regarding the Applicability of Safe Harbor. The following discussion is contained in Section 6 of The SAR Activity Review – Trends, Tips & Issues (June 2001).

© gettechnical inc 2021

Answer 11: The safe harbor provisions applicable to SAR filings provide a safe harbor for organizations that provide a SAR to all authorized government personnel, including Federal, state, and local authorities. Similarly, the safe harbor provisions apply even if the report of activity that is a possible violation of law or regulation is made orally or in some form other than through the use of a SAR. (6/2001)

Question 12a: A business customer of a depository institution provides payroll checks to individual employees for work performed. Each payroll check is under $10,000. However, several employees cash their payroll checks individually on the same business day, which results in an aggregate cash out from the business customer's account in an amount exceeding $10,000. Would the institution be required to file a CTR, if no one person received an amount in excess of $10,000?

Answer 12a: The financial institution would not need to file a CTR because it would not be involved in a single cash transaction (or multiple cash transactions for which a duty to aggregate would arise) of more than $10,000. A financial institution must treat multiple transactions in currency as a single transaction if the financial institution has knowledge that the multiple transactions are "by or on behalf of any person" and result in cash in or cash out totaling more than $10,000 during any one business day. According to the facts described above, the cashing of checks would be conducted by or on behalf of each individual employee (rather than the business on whose account each check is drawn), and no one employee would be cashing more than $10,000 in a single transaction or in multiple transactions during the same business day.

Question 13b: Would a CTR be required if several individual employees endorsed their respective payroll checks (all individual payroll checks are under $10,000 but combined they aggregate to an amount that exceeds $10,000), and made the checks payable to one employee who, in turn, cashed them at a financial institution for the purpose of distributing the proceeds back to the individual employees?

Answer 13b: A CTR would be required in this instance because one person is receiving more than $10,000 in currency. (10/2001).

Question 13c: Is a CTR required when a person presents a check, in excess of $10,000, for payment in cash at a financial institution and receives less than $10,000 after fees, or other deductions, are charged against the amount of the check?

Answer 13c: The BSA only requires a CTR for a transaction in currency, such as a deposit, withdrawal, exchange or transfer of currency, in excess of $10,000. A transaction in currency involves the physical transfer of currency from one person to another. Accordingly, the transfer of currency below $10,000 would not trigger the CTR requirement, despite the amount of the check. For example, if a person cashed a check for $10,100 and received $9,990 after a service fee was charged against the amount of the check, the financial institution would not be required to file a CTR. On the other hand, if a person purchased a cashier's check for $9,990 and paid a service fee of $20 for a total of $10,010 in cash, the financial institution would be required to file a CTR. The key lies in

© gettechnical inc 2021

the amount of the physical deposit, withdrawal, exchange or transfer of currency. (10/2001).

Question 14: Is a state-licensed check-cashing business exemptible under the BSA?

Answer 14: The CTR exemption regulations do not distinguish between a "licensed" or "non-licensed" business. In determining whether any check-cashing business is eligible for exemption from currency transaction reporting requirements, a depository institution must determine whether the business falls into either of two categories described below: (12/2017)

1. An entity listed on one of the major national stock exchanges, or a subsidiary of an entity listed on those stock exchanges as described in 31 CFR § 1020.315). If a customer falls under one of the categories identified in 31 CFR § 1020.315, the depository institution does not need to determine if the business activity is considered ineligible for exemption as identified in 31 CFR § 1020.315(e)(8). Once the depository institution has determined that the customer qualifies for an exemption based on the above criteria, the depository institution may file a one-time DEP form.

2. A non-listed business, if the criteria of 31 CFR § 1020.315 are met. Determining if a business can be considered a non-listed business depends, in part, on whether the customer is primarily engaged in one or more of the ineligible business activities listed in 31 CFR § 1020.315. If primarily engaged in such ineligible business activities, then the customer cannot be treated as a non-listed business.

a. One of the ineligible business activities listed in 31 CFR § 1020.315 is serving as a financial institution. Under the BSA, the definition of "Financial Institution" includes money services businesses (MSBs) [31 CFR 1010.100(ff)]. A check casher is defined as an MSB if it cashes checks in an amount greater than $1,000 in currency or monetary instruments for any one person in any one day in one or more transactions [31 CFR 1010.100(ff)(2)]. Consequently, if the check casher meets the definition of an MSB, it is considered to be serving as a financial institution. Therefore, if the check casher is defined as an MSB and is primarily engaged (see item b. below) in the business of cashing checks [or other ineligible business activity listed in 31 CFR § 1020.315, then it is ineligible for treatment as an exempt person.

b. If a business engages in multiple business activities (e.g., money transmission in addition to check cashing), it may be treated as a non-listed business so long as no more than 50% of its gross revenues is derived from one or more of the ineligible business activities listed in § 1020.315.

Example 1: A check casher (whether licensed or non-licensed) that cashes checks in an amount less than $1,000 in currency or monetary instruments for any one person on any one day and is not involved in any other ineligible business activity, or derives no more than 50% of its gross revenue from any such business, may be exempted from CTR reporting requirements as a non-listed business (assuming that all other criteria listed in 31 CFR § 1020.315 are met).

© gettechnical inc 2021

Example 2: A check casher (whether licensed or non-licensed) that cashes checks in an amount more than $1,000 in currency or monetary instruments for any one person on any one day and derives more than 50% of its gross revenue from cashing checks (and/or other ineligible business activity) may not be exempted from CTR reporting requirements as a non-listed business because it is serving as a financial institution under the BSA regulations.

Question 15: Does FinCEN prepare and distribute training materials, such as videos, on the BSA reporting and recordkeeping requirements?

Answer 15: FinCEN does not currently prepare or distribute training videos or materials. FinCEN frequently participates in conferences and other forums to discuss BSA reporting and recordkeeping requirements, developments relating to FinCEN's regulations, and counter money laundering efforts.

FinCEN's publications also impart information that may be useful in the preparation of training materials, such as SAR Guidance, Strategic Analytical Reports, and The SAR Activity Review: Trends, Tips & Issues, which are available on FinCEN's web site under the tab for "Reports & Publications". FinCEN also frequently issues guidance to financial institutions on BSA reporting and recordkeeping requirements.

Furthermore, financial institutions, particularly depository institutions such as banks, thrifts and credit unions, have significant resource materials available to help them train from their industry associations and other sources in the private sector. In addition, the primary regulators may also provide publications and resource material to use in BSA training and may be consulted on BSA compliance issues.(10/2001).

Question 16: When a Federal, state or local government official, as part of his or her official duties, engages in a transaction in currency over $10,000, or purchases a monetary instrument for more than $3,000 in currency, as a non-accountholder, what kind of identifying information must a financial institution obtain?

Answer 16: Government officials sometimes need to conduct large currency transactions as part of their official duties. For example, a law enforcement official may wish to convert seized currency into monetary instruments for security reasons. Banks are not required to file a CTR when a Federal, state or local government official, as part of his or her official duties, engages in a transaction in currency over $10,000. In addition, banks do not need to file a Designation of Exempt Person form (FinCEN Form 110) for customers that are a department or agency of the United States, of any State, or of any political subdivision of any State. A bank should, however, take the steps to ensure that the customer is eligible for the exemption (that the customer is a government official conducting business on behalf of a government agency) and document the basis for that determination (e.g., reviewing the customer's law enforcement credentials or government photo ID).

Notwithstanding the above, a financial institution should still obtain and record the name of the government official conducting the transaction. Regarding the purchase of a monetary instrument for more than $3,000 in currency, a financial institution should record the name

© gettechnical inc 2021

and date of birth of the government official, for the financial institution's records. (12/2017)

Questions 17: Can you provide guidance on how money services businesses should conduct independent reviews of their anti-money laundering programs?

Answer 17: There are frequently asked questions regarding how to conduct independent reviews on money services business anti-money laundering programs. FinCEN has issued the following guidance 1.

The Bank Secrecy Act requires money services businesses to establish anti-money laundering programs that include "an independent audit function to test programs." In implementing this requirement, we determined to make clear that money services businesses are not required to hire a certified public accountant or an outside consultant to conduct a review of their programs. Rather, the relevant Bank Secrecy Act regulation requires money services businesses to establish anti-money laundering programs with written policies and procedures that:

Provide for independent review to monitor and maintain an adequate program. The scope and frequency of the review shall be commensurate with the risk of the financial services provided by the money services business. Such review may be conducted by an officer or employee of the money services business so long as the reviewer is not the person designated in paragraph (d)(2) of this section.

The primary purpose of the independent review is to monitor the adequacy of the money services business' anti-money laundering program. The review should determine whether the business is operating in compliance with the requirements of the Bank Secrecy Act and the business' own policies and procedures. Each money services business should identify and assess the money laundering risks that may be associated with its unique products, services, customers, and geographic locations. Regardless of where risks arise, money services businesses must take reasonable steps to manage them. Each money services business should focus resources on the areas of its business that management believes pose the greatest risks, and the level of sophistication of the associated internal controls should be appropriate for the size, structure, risks, and complexity of the money services business.

Question 18(a): What should be done during the review? The review should provide a fair and unbiased appraisal of each of the required elements of the company's anti-money laundering program, including its Bank Secrecy Act-related policies, procedures, internal controls, recordkeeping and reporting functions, and training.

Answer 18(a): The review should include testing of internal controls and transactional systems and procedures to identify problems and weaknesses and, if necessary, recommend to management appropriate corrective actions. For example, if the program requires that a particular employee or category of employee should be trained once every six months, then the independent testing should determine whether the training occurred and whether the training was adequate.

© gettechnical inc 2021

The review also should cover all of the anti-money laundering program actions taken by – or defined as part of the responsibility of – the designated compliance officer. These actions include, for example, the determination of the level of money laundering risks faced by the business, the frequency of Bank Secrecy Act anti-money laundering training for employees, and the adoption of procedures for implementation and oversight of program-related controls and transactional systems.

Question 18(b): Who should conduct the review?

Answer 18(b): Our regulations require an independent review, not a formal audit by a certified public accountant or third-party consultant. Accordingly, a money services business does not necessarily need to hire an outside auditor or consultant. The review may be conducted by an officer, employee or group of employees, so long as the reviewer is not the designated compliance officer and does not report directly to the compliance officer.

Question 18(c): How often should the review occur?

Answer 18(c): The review should be conducted on a periodic basis. The scope and frequency of the review will depend on the money services business' risk assessment, which should take into account the business' products, services, customers, and geographic locations. For some money services businesses, based on their risk assessments, an annual review may not be necessary; for others, more frequent review may be warranted. For example, if the money services business' risk assessment changes, more frequent review may be prudent. Similarly, if compliance problems are identified in a review, it may be advisable to advance the date of the next review to confirm that corrective actions have been taken.

Question 18(d): Should the review be documented in some manner and reported to management?

Answer 18(d): Yes. The person or persons responsible for conducting the review should document the scope of the review, procedures performed, transaction testing completed, if any, findings of the review, and recommendations to management for corrective actions, if any. After the review, the reviewer or the designated compliance officer should track deficiencies and weaknesses discovered during the review and document corrective actions taken by the money services business. All of the documentation should, as appropriate, be made accessible to government examiners and law enforcement personnel who have authority to examine such documents. (9/2006)

© gettechnical inc 2021

http://www.fincen.gov/whatsnew/html/sar_faqs.html

Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (SAR)

1. What are the expectations for completing the Items with an asterisk ("critical") and without an asterisk ("non-critical") found on the FinCEN SAR or any other FinCEN report?

As explained in FinCEN's March 2012 guidance (FIN-2012-G002), for both critical and non-critical elements, financial institutions should complete those Items for which they have relevant information, regardless of whether or not the individual Items are deemed critical for technical filing purposes.

For critical Items, financial institutions must either provide the requested information or affirmatively check the "Unknown" (Unk.) box that is provided on the FinCEN SAR and FinCEN Currency Transaction Report (CTR) (or any other FinCEN Report).

For non-critical Items, FinCEN expects financial institutions will provide the most complete filing information available within each report consistent with existing regulatory expectations. Based upon feedback from law enforcement officials, such information is important for query purposes. However, the new FinCEN SAR and FinCEN CTR do not create any new obligations to collect data, either manually or through an enterprise-wide IT management system, where such collection is not already required by current statutes and regulations, especially when such collection would be in conflict with the financial institution's obligations under any other applicable law. Therefore, a financial institution may leave non-critical fields without an asterisk blank when information is not readily available.

2. How do I meet my underlying obligation to submit a complete and accurate report if my filing software does not allow me to include known information for a field without an asterisk?

FinCEN expects financial institutions to have the capability to submit information for any of the data fields in the FinCEN SAR or CTR (or any other FinCEN report). In general, if your financial institution's filing software does not permit the institution to include information in a field without an asterisk where information has been collected and is pertinent to the report, the financial institution should instead complete a discrete filing for those transactions until the software is updated. If a filing has been submitted in which such information was not included because of such a limitation in the filing software, an

© gettechnical inc 2021

amended filing should be completed using either the discrete filing method or an amended batch filing, once the software is updated. Such software updates should be implemented within a reasonable period of time.

If your institution has questions regarding the applicability of this general guidance, please contact the FinCEN Regulatory Helpline at (800) 949-2732 for further information.

3. When I log into BSA E-Filing, I do not see the new FinCEN SAR.

"General users" of the Bank Secrecy Act (BSA) E-Filing System can only view those reports that the "supervisory user" has given them permission to see. If you cannot view or access the new FinCEN SAR, please contact your supervisory user to request access.

Supervisory users of the BSA E-Filing System are able to view all available FinCEN reports when they log into the BSA E-Filing System. The supervisory user must grant access for the general users to be able to view the new FinCEN reports.

To do so, a supervisory user first must:

1. Log into the BSA E-Filing System.

2. Select "Manage Users" from the left-hand side under "User Management."

3. Select the general user whose access roles require updating.

4. Select "Reassign Roles."

Upon reaching the next webpage, the supervisory user must:

1. Select the roles ("FinCEN SAR Filer," "FinCEN SAR Batch Filer," "FinCEN CTR Filer," "FinCEN CTR Batch Filer," "FinCEN DOEP Filer," "FinCEN DOEP Batch Filer," etc.) in the "Remaining Roles" box that need to be added for the general user.

2. Move those selected roles to the "Current Roles" box and select "Continue."

After all these steps are completed, the general user will now have access to the selected new roles and can access the new FinCEN reports.

4. Where can I find the instructions for completing the new FinCEN SAR?

Electronic filing instructions can be found in Attachment C of the "FinCEN SAR Electronic Filing Requirements" document. This document can be found under "User Quick Links" of the BSA E-Filing System homepage (http://bsaefiling.fincen.treas.gov/main.html) or on the "Forms" page of the FinCEN Web site (http://www.fincen.gov/forms/bsa_forms/).

© gettechnical inc 2021

Additionally, instructions are embedded within the discrete filing version of the FinCEN CTR and are revealed when scrolling over the relevant fields with your computer "mouse."

5. What do I enter for "Filing Name"?

The filing name can be any name the financial institution chooses to use to identify the specific filing (e.g., Bank SAR 4-4-2013). The process for assigning filing names is for the financial institution to decide, and can assist the financial institution in tracking its BSA filings. We recommend using a naming convention that will be easy to understand and track for recordkeeping and audit/examination purposes. FinCEN strongly recommends, however, that FinCEN SAR file names not include the names of subjects as this may lead to the inappropriate disclosure of the SAR, which is prohibited by law and regulation.

6. How do I file a corrected/amended FinCEN SAR via the BSA E-Filing System?

Filers attempting to submit a corrected/amended SAR via the BSA E-Filing System should check "Correct/amend prior report" and enter the previous Document Control Number (DCN)/BSA Identifier (ID) in the appropriate field. The filer should complete the FinCEN SAR in its entirety, including the corrected/amended information and noting those corrections at the beginning of the narrative, save (and print, if desired) a copy of the filing, and submit the filing. The corrected/amended FinCEN SAR will be assigned a new BSA ID.

To find your DCN/BSA ID for the previous filing, you will need the acknowledgement received by the general user after successfully submitting the report into the BSA E-Filing System. All general users assigned access to the new FinCEN reports automatically receive these acknowledgements. Filers can choose to receive these acknowledgements in an "ASCII" or "XML" format. Please also note that supervisory users cannot view the contents of the acknowledgements received by the general users.

7. How do I correct/amend a prior SAR filing via the BSA E-Filing System if I do not have the prior DCN/BSA ID?

If the previous DCN/BSA ID is not known, filers should enter all "zeros" (14 in total) for the previous DCN/BSA ID. This information was published in a Notice on October 31, 2011. This notice is applicable to corrections/amendments for any previous filing. The filer should complete the FinCEN SAR in its entirety, including the corrected/amended information and noting those corrections at the beginning of the narrative, save (and print, if desired) a copy of the filing, and submit the filing. The corrected/amended FinCEN SAR will be assigned a new BSA ID that will be sent to the filer in the FinCEN SAR acknowledgement. The new BSA ID will begin with the number "31."

8. Can we obtain a copy of a FinCEN SAR that we filed using the BSA E-Filing System?

The BSA E-Filing System is not a record keeping program; consequently, filers are not able to access or view previously filed reports. The BSA E-Filing System does provide

tracking information on past report submissions and acknowledgements for accepted BSA reports. Users of the BSA E-Filing System must save and can print a copy of the FinCEN SAR prior to submitting it. FinCEN does not provide copies of filed reports to filers.

9. When should I save the copy of the FinCEN SAR that is being filed using the BSA E-Filing System?

A BSA filing may be saved at any stage of completion and then reopened at a later time to complete and submit into the BSA E-Filing System. You must electronically save your filing before it can be submitted into the BSA E-Filing System. ***NOTE: The BSA E-Filing System is not a record keeping program.*** When saving a BSA filing, users must save the filing to their computer, network, or other appropriate storage device. For additional information about recordkeeping requirements under the BSA, please refer to 31 CFR § 1010.430 and FAQ #11.

Please note that the BSA E-Filing System will log filers off the system after a certain time period if there is no action within the account, even if the filer is working within the FinCEN SAR. For that reason, FinCEN strongly recommends that filers download the FinCEN SAR template, log out of BSA E-Filing, complete the FinCEN SAR off-line, and then log back into BSA E-Filing to upload and submit the report.

10. Where can I save a report being filed electronically??

A filer can electronically save the filing to his/her computer hard drive, a network drive, or other appropriate storage device. By clicking on the "Save" button a standard dialog box will appear to allow you to choose the location for your saved report. Once the report is saved, the "Submit" button will become available. A filer may also want to print a paper copy for your financial institution's records.

A filer should NOT save a copy of the report on a public computer or a computer that is not regularly accessed by the filer. This will ensure that the file remains appropriately secured.

11. What are my recordkeeping requirements when I submit a file electronically?

After submitting a report via the BSA E-Filing System, filers are required to save a printed or electronic copy of the report in accordance with applicable record retention policies and procedures. Filers are reminded that they are generally required to keep copies of their filings for five years. See 31 CFR § 1010.306(a)(2), 31 CFR § 1010.330(e)(3), 31 CFR § 1010.340(d), 31 CFR § 1020.320(d), 31 CFR § 1021.320(d), 31 CFR § 1022.320(c), 31 CFR § 1023.320(d), 31 CFR § 1024.320(c), 31 CFR § 1025.320(d), 31 CFR § 1026.320(d), 31 CFR § 1029.320(d), and 31 CFR § 1022.380(b)(1)(iii).

12. What are the steps for properly submitting a single (discrete) FinCEN SAR filing through the BSA E-Filing System

© gettechnical inc 2021

Please ensure all of the following steps are followed when completing a single FinCEN SAR:

1. Complete the report in its entirety with all requested or required data known to the filer.

2. Click “Validate” to ensure proper formatting and that all required fields are completed.

3. Click “Sign with PIN” – Enter the personal identification number (PIN) the BSA E-Filing System has assigned to your user ID. If you do not know your PIN, please click on the “Manage PIN” link in the left navigation menu for your PIN to be displayed.

4. Click “Save” – Filers may also “Print” a paper copy for their records. The “Save” button will allow you to select the location to save your filing.

5. Click “Submit” – After clicking “Submit,” the submission process will begin.

13. How can I validate that my discrete filing submission was accepted properly by the BSA E-Filing System?

After clicking “Submit,” the submission process begins. Once your filing is accepted into the BSA E-Filing System, a “Confirmation Page” pop-up will appear with the following information:

- Tracking ID (A unique tracking ID assigned to the filing by BSA E-Filing)
- Date and time of the submission
- Submission Type
- Owner (submitter) Name
- Owner (submitter) email address
- Filing Name

An email will also be sent to the email address associated with your BSA E-Filing account indicating your submission has been “Accepted” for submission into the BSA E-Filing System. .

If the Confirmation Page pop-up is not displayed, your filing was not accepted for submission by the BSA E-Filing System. If you are returned to the BSA E-Filing System login page, your connection has timed out and you must login to the BSA E-Filing System and resubmit your report. It is recommended that you first close out of your browser and then re-open it before attempting to log into the BSA E-Filing System again.

Once your report is accepted and a confirmation page pop-up is displayed, the status of your report can be viewed by clicking on the “Track Status” link on the left navigation menu. The status will appear as “Accepted.”

Within 48 hours, your report will be formally acknowledged as having been successfully processed for inclusion in FinCEN’s data base. The status will change to “Acknowledged”

© gettechnical inc 2021

in the “Track Status” view. In addition, a secure message containing the official BSA ID assigned to your report will be sent to your “Secure Mailbox.”

FAQs associated with Part I of the FinCEN SAR

14. Why are the numbers on the fields in the FinCEN SAR out of order

When initially published for public comment, the FinCEN SAR was structured and numbered consistent with the overall format for all the new FinCEN Reports, to include multiple Parts and beginning with the information about the persons involved in the transactions. As a result, the FinCEN SAR starts the numbering of line items on the initial “submission” page as with all the other reports, and continues the numbering in the order of Parts I, II, III, IV, and V, with some minor exceptions.

To accommodate better the dynamic nature of the report, FinCEN determined that it would be more helpful for the filing institution information in Part IV and Part III to be completed before moving to the description of the suspect and the suspicious activity. In doing so, this shifted the order of the Office of Management and Budget (OMB)-approved fields and their associated numbers within the FinCEN SAR.

While the ordering may initially be confusing, there is a significant benefit to the filer in completing Parts IV and III first. By identifying the filer’s institution type (depository institution, broker-dealer, MSB, insurance, etc.), name of the institution, the filer’s financial institution identification number (e.g., Research, Statistics, Supervision, and Discount or RSSD)/Employer Identification Number (EIN), and its address, the report enables or ‘‘auto populates’’ certain data elements elsewhere in the report. The institution can then complete the specific information on the subject(s) and nature of the suspicious activity using the data elements that have been enabled as most appropriate to its type of financial institution. In the case of a report filed jointly by two or more financial institutions, all data elements will be available for selection. Should a single filer require access to additional elements not typical for the filer’s type of financial institution, the filer can enable those other data elements for selection.

15. How do I determine whether or not to indicate a North American Industry Classification System (NAICS) Code?

FinCEN previously issued guidance in March 2012 that addressed the selection of the NAICS Code on the FinCEN SAR and FinCEN CTR. FinCEN emphasized that financial institutions will continue to be expected to provide only that information for which they have direct knowledge. As noted in that guidance, the issuance of the FinCEN SAR does not create any new obligation or otherwise change existing statutory and regulatory requirements for the filing institution. In addition, use of a NAICS code is not mandatory, and a financial institution may still provide a text response with respect to this information within the “Occupation” field.

© gettechnical inc 2021

Please note that batch filers must use only the 3-4 digit NAICS codes on our approved list of codes. Discrete filers can select from the available drop-down list embedded within the SAR.

Please refer to FIN-2012-G002 for further information.

FAQs associated with Part II of the FinCEN SAR

16. What is the filing timeframe for submitting a continuing activity report?

FinCEN provided clarifying guidance on this question in Section 4 (Page 53) of SAR Activity Review Trends, Tips, & Issues #21. The guidance states "Financial institutions with SAR requirements may file SARs for continuing activity after a 90-day review with the filing deadline being 120 days after the date of the previously related SAR filing. Financial institutions may also file SARs on continuing activity earlier than the 120-day deadline if the institution believes the activity warrants earlier review by law enforcement."

So, for filings where a subject has been identified, the timeline is as follows:

- Identification of suspicious activity and subject: Day 0.
- Deadline for initial SAR filing: Day 30.
- End of 90 day review: Day 120.
- Deadline for continuing activity SAR with subject information: Day 150 (120 days from the date of the initial filing on Day 30).
- If the activity continues, this timeframe will result in three SARs filed over a 12-month period.

17. The FinCEN SAR does not include the suspicious activity characterization of "computer intrusion" that was provided in the legacy SAR-DI. Is that definition still valid? How does it differ from "account takeover" and how should I apply previous FinCEN guidance on this topic within the FinCEN SAR?

For purposes of the FinCEN SAR, the term "computer intrusion" has been replaced by the term "unauthorized electronic intrusion"; but that new term continues to be defined as gaining access to a computer system of a financial institution to:

a. Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers.

b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information.

c. Damage, disable or otherwise affect critical systems of the institution.

For purposes of this reporting requirement, unauthorized electronic intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information.

© gettechnical inc 2021

Please note: the term “unauthorized electronic intrusion” does not include incidents that temporarily interrupt or suspend online services, which are commonly referred to as “Distributed Denial of Service (DDoS)” attacks. FinCEN intends to issue further guidance on the reporting of DDoS attacks.

When completing the FinCEN SAR on activity that previously would have been identified as “computer intrusion,” financial institutions now should check 35q “Unauthorized electronic intrusion.” Since more than one type of suspicious activity may apply, the financial institutions should check all boxes that apply when completing Items 29 through 38. In addition, financial institutions should provide a detailed description of the activity in the narrative section of the SAR.

“Account takeover” activity differs from other forms of computer intrusion, as the customer, rather than the financial institution maintaining the account, is the primary target. In an account takeover, at least one of the targets is a customer holding an account at the financial institution and the ultimate goal is to remove, steal, procure or otherwise affect funds of the targeted customer.

The following explains how to apply the guidance provided in FinCEN advisory FIN-2011-A016 when using the FinCEN SAR:

- Financial institutions should select box 35a (Account takeover) to report that type of suspicious activity. If the account takeover involved computer intrusion/unauthorized electronic intrusion, institutions also should check box 35q (Unauthorized electronic intrusion).
- If the account takeover involved other delivery channels such as telephone banking or fraudulent activities such as social engineering, financial institutions can check box 35a (Account takeover) and other appropriate suspicious activity characterizations; for example, the involvement of mass marketing fraud could be identified by checking box 31h.
- If the account takeover involved a wire transfer, then in addition to selecting box 35a (Account takeover), box 31j for "Wire fraud" should be checked.
- If the account takeover involved an ACH transfer, financial institutions should select box 35a (Account takeover) and box 31a for “ACH fraud.”
- Account takeovers often involve unauthorized access to PINs, account numbers, and other identifying information. Financial institutions may need to check box 35g for "Identity theft," in addition to selecting box 35a (Account takeover).
- In addition to the above guidance, financial institutions should select any other characterization boxes appropriate to the identified suspicious activities (e.g., box 30a or 30z for "Terrorist financing"). If there is other related activity for which there is not a clear characterization selection, check box 31z (Other) if the activity is related to fraud or box 35z (Other) if it is related to other suspicious activity. Include a short description of the additional information in the space provided with those selections.

FAQs associated with Part III of the FinCEN SAR

© gettechnical inc 2021

18. How do we complete Item 52/64 on the new FinCEN SAR which asks for the financial institution or branch's "role in transaction," and provides options for "Selling location," "Paying Location," or "Both"?

The new FinCEN SAR is a "universal" SAR as it combines elements from the various legacy SAR forms that FinCEN previously issued. While Items 52 and 64 were elements of the legacy "SAR-MSB," they may be applicable to other types of financial institutions, providing useful information to law enforcement. Items 52 and 64 are non-critical fields, however, and only need to be completed if they are applicable to the activity being reported. As an example, if the activity being reported on the FinCEN SAR involved only the structuring of cash deposits, then a financial institution would not complete Items 52 or 64, as the institution was neither a "paying" nor "selling" location in the activity being reported. As another example, if the activity being reported on the FinCEN SAR involved unauthorized pooling of funds, then a financial institution would not complete Items 52 or 64, as the institution was neither a "paying" nor a "selling" location in the activity being reported.

On the other hand, if the activity being reported on the FinCEN SAR involved the suspicious purchasing of cashier's checks by a customer, then a financial institution would check Item 40a "Bank/Cashier's check," and use Item 52 to indicate that the filing institution was the "Selling location." If the sale of cashier's checks included activity occurring at branch locations, then in completing the section for "Branch where activity occurred," the financial institution would use Item 64 to identify the additional branches as "Selling location(s)" for the customer cashier's checks. To add additional branches to the FinCEN SAR, click on the "+" icon to bring up additional sections in which to include the information related to those branches.

The "Webinar on the FinCEN SAR" located on the "Financial Institutions" homepage of www.fincen.gov provides additional examples of the appropriate use of these fields.

19. I represent a depository institution and I would like to know my financial institution identification type on the SAR. Do I include the branch level or financial institution level information?

A depository institution would select the Research, Statistics, Supervision, and Discount (RSSD) number. You can find your institution's RSSD number at http://www.ffiec.gov/nicpubweb/nicweb/nichome.aspx or http://www.ffiec.gov/find/callreportsub.htm.

You would include the RSSD number associated with the "Filing Institution" in Item 84 (Part IV) and that of the "Financial Institution Where Activity Occurred" in Item 51, which could be a branch location. When the activity being reported occurs at additional branch locations, you should include the RSSD number associated with the additional branch(s) in Item 66

If the branch location at which the activity occurred does not have an RSSD number, however, leave that Item blank. This may occur if an RSSD number has not yet been issued

for a new branch, but we expect few depository institutions to not have an RSSD for each branch. If the branch has the same RSSD number as the financial institution as a whole, you should use the overall financial institution RSSD number. This will occur with credit unions.

Please note that it is important to have the information within the filing regarding the branch or other location at which the activity occurred as complete and accurate as possible. This greatly assists law enforcement in understanding where the activity occurred.

FAQs associated with Part IV of the FinCEN SAR

20. What information should be provided in Items 78 – 90 in Part IV of the FinCEN SAR

Part IV records information about the lead financial institution, holding company, agency, or other entity that is filing the FinCEN SAR. Below are examples of how Part IV would be completed in various scenarios.

a. A Bank Holding Company (BHC) has implemented an enterprise-wide approach to their compliance program. As a result, the BHC will file all required reports with FinCEN. In this scenario, Part IV would be completed with the information of the BHC, and then a Part III would be completed with the information of the financial institution where the activity occurred. If the activity occurred at additional branch locations, then that information would be entered in Items 64 – 70, and would be repeated as many times as necessary. In Part IV, the filing institution should enter the name of the office that should be contacted to obtain additional information about the report.

b. A single depository institution with multiple branches files their SARs out of the home office of the depository institution. In this scenario, Part IV would be completed with the information of the home office of the depository institution, and then a Part III would be completed for the depository institution location where the activity occurred. If the activity occurred at additional branch locations of the depository institution, then that information would be entered in Items 64 – 70, and would be repeated as many times as necessary. In Part IV, the filing institution should enter the name of the contact office that should be contacted to obtain additional information about the report.

c. A depository institution and a money services business (MSB) decide to file a joint SAR together, agreeing that the depository institution would file the SAR. Part IV would be completed with the information of the depository institution that is filing the SAR. A Part III would be completed for the depository institution's locations where the activity occurred. If the activity occurred at additional branch locations of the depository institution, then that information would be entered in Items 64 – 70, and would be repeated as many times as necessary.

In addition, a Part III would be completed for the MSB's location where the activity occurred. If the activity occurred at additional branch locations of the MSB, then that

© gettechnical inc 2021

information would be entered in Items 64 – 70, and would be repeated as many times as necessary.

The filing institution listed in Part IV "Filing Institution Contact Information" must identify in Part V "Suspicious Activity Information – Narrative" which of the Part III "Financial Institution Where Activity Occurred" institutions are the joint filers. The filing institution must include joint filer contact information in Part V, along with a description of the information provided by each joint filer. In Part IV, the filing institution should enter the name of the office that should be contacted to obtain additional information about the report. If a joint SAR is being prepared, please refer to General Instruction 5 "Joint Report" for additional instructions.

Please note that a branch is a location (such as an office or ATM) owned by the financial institution but located separately from the financial institution's headquarters. If a reporting financial institution has agents where the suspicious activity occurred, a separate Part III must be prepared on each agent. An agent is an independent financial institution (such as a supermarket that sells money orders or an independent insurance agent) that has a contractual relationship with the reporting financial institution to conduct financial transactions. Do not place agent information in branch fields.

21. Item 96 now asks for a contact office and not a contact person. What information should be provided in this field?

The filing institution should enter the name of the office that should be contacted to obtain additional information about the report. It is the filing institution's choice as to which office this should be. Examples may include "Compliance Office," "Security Office," "BSA Office," or "Risk Management Office." The office may or may not be located at the location identified in the same Part IV.

22. Item 97 asks for the filing institution's contact phone number. Should this be the number associated with the contact office noted in Item 96?

Yes, the filing institution's contact phone number should be the phone number of the contact office noted in Item 96.

Additional questions or comments regarding these FAQs should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

© gettechnical inc 2021

FinCEN FIN-2018-A003: Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators (6/12/2018)

UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

ADVISORY

FIN-2018-A003 June 12, 2018

Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operations Officers*
- *Chief Risk Officers*
- *Legal Departments*
- *Chief Compliance/BSA Officers*
- *AML Officials*
- *Sanctions Compliance Officials*

The U.S. Department of the Treasury (Treasury) is committed to protecting both the U.S. and international financial systems, not only from those who engage in corruption and human rights abuses, but from those who facilitate such activities as well. High-level political corruption undermines democratic institutions and public trust, damages economic growth, and fosters a climate where financial crime and other forms of lawlessness can thrive. Corrupt senior foreign political figures, their subordinates and facilitators, through their corrupt actions, often contribute directly or indirectly to human rights abuses, which have a devastating impact on individual citizens and societies, undermining markets and economic development and creating instability in a region. The use of financial facilitators is one way that corrupt senior foreign political figures access the U.S. and international financial system to move or hide illicit proceeds, evade U.S. and global sanctions, or otherwise engage in illegal activity, including related human rights abuses.

Treasury employs its unique tools, consistent with applicable authorities, to impose financial consequences on those who pillage the wealth and resources of their people, generate ill-gotten profits from corruption, cronyism, and other criminal activity, and engage in human rights abuses. These tools include the ability to sanction corrupt actors and human rights abusers around the world under an Executive Order implementing the Global Magnitsky Act of 2016,[1] taking enforcement action against financial facilitators of corrupt senior foreign political figures, as well as issuing advisories to financial institutions to help them identify, mitigate, and report on these risks. Treasury will also continue to partner with others that are active in this area, such as the U.S. Department of Justice, the Financial Action Task Force (FATF), civil society, and non-governmental organizations (NGOs) to identify, constrain, and deprive corrupt actors and those who support their access to financial systems.

1. *See* Executive Order 13818, "Blocking the Property of Persons Involved in Serious Human Rights Abuse and Corruption," December 20, 2017; *see also* United States Sanctions Human Rights Abusers and Corrupt Actors Across the Globe December 21, 2017.

© gettechnical inc 2021

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to U.S. financial institutions to highlight the connection between corrupt senior foreign political figures and their enabling of human rights abuses. The advisory describes a number of typologies used by them to access the U.S. financial system, obscure, and further their illicit activity. The advisory also provides red flags that may assist financial institutions in identifying the methods used by corrupt senior foreign political figures,[2] including the use of facilitators, to move and hide the proceeds of their corruption, which contribute directly or indirectly to human rights abuses or other illicit activity, through the U.S. financial system.

FinCEN will update these red flags and typologies as it continues investigating the methodologies associated with corrupt senior foreign political figures and their financial facilitators. This advisory also reminds U.S. financial institutions of their due diligence and suspicious activity report (SAR) filing obligations related to such corrupt senior foreign political figures and their financial facilitators.

Targeted Financial Sanctions against Corruption and Human Rights Abuse

Treasury's Office of Foreign Assets Control (OFAC) has a range of authorities to designate corrupt senior foreign political figures, human rights abusers and their financial facilitators. OFAC has numerous country sanction programs, including those for Venezuela, South Sudan, Iran, Russia, Syria, the Democratic Republic of the Congo (DRC), North Korea, and Somalia, that allow OFAC to broadly prohibit U.S. persons, including U.S. financial institutions, from engaging in transactions involving designated individuals and entities that have engaged in corruption, undermined democratic processes, or engaged in human rights abuse. All assets of the designated individuals and entities subject to U.S. jurisdiction are frozen and U.S. persons, including U.S. financial institutions, are prohibited from dealing with the designated person.[3]

2. The term "senior foreign political figure" means a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not); a senior official of a major foreign political party; or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity that has been formed by, or for the benefit of, any such individual; an immediate family member of any such individual; and a person who is widely and publicly known (or is actually known by the relevant covered financial institution) to be a close associate of such individual. 31 CFR § 1010.605(p). For the purposes of this definition, "senior official or executive" means an individual with substantial authority over policy, operations, or the use of government-owned resources and 'immediate family member' means spouses, parents, siblings, children and a spouse's parents and siblings. 31 CFR § 1010.605(p). *See also generally* 31 CFR § 1010.620. Note that the term "senior foreign political figure" connotes a subset within the concept of "politically exposed persons" (PEPs). The term PEP is not included in FinCEN's regulations and should not be confused with "senior foreign political figure." In the United States, AML obligations with respect to PEPs collectively include 1) the specific enhanced due diligence obligations for private banking accounts that are established, maintained, administered, or managed in the United States for senior foreign political figures, and 2) the general due diligence procedures required for all politically exposed persons, incorporated into the institution's anti-money laundering program as appropriate. *See* SAR Activity Review Trends, Tips, and Issues: Issue 19 May 2011.

3. *See* OFAC Website, Sanctions Programs and Country Information.

© gettechnical inc 2021

The Global Magnitsky sanctions program provides Treasury with a powerful tool for targeting corrupt officials, human rights abusers, and corrupt actors and their facilitators, regardless of the country in which they reside or where they operate.[4] The Global Magnitsky Executive Order empowers OFAC to cut off from the U.S. financial system any person determined by the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, to be, among other things, engaging in human rights abuse, or engaging in corruption. The prohibitions of Global Magnitsky can extend to those who provide goods or services to such actors, including financial institutions.

Financial Action Task Force Initiatives and Recommendations Related to Politically Exposed Persons (PEPs)

To address the financial risks associated with PEPs, the FATF issued Recommendation 12, which requires countries to ensure that financial institutions implement measures to prevent the misuse of the financial system by PEPs and to detect such potential abuse, if and when it occurs.[5] The FATF recommends that family members and close associates of PEPs should be considered PEPs because of the potential for abuse of the relationship for the purpose of moving the proceeds of crime, facilitating placement and disguise of the proceeds, as well as for terrorist financing purposes.[6]

In the United States, Recommendation 12 is implemented through FinCEN rules and guidance and complemented by supervisory expectations articulated in the Federal Financial Institutions Examination Council (FFIEC) BSA Examination Manual. Among other things, with regard to foreign PEPs, banks should exercise reasonable judgment in designing and implementing policies, procedures, and processes regarding foreign PEPs as a part of their anti-money laundering (AML) program. This could include obtaining risk-based due diligence information on PEPs, such as countries of residence of the accountholder(s) and beneficial owner(s) and the level of corruption and money laundering risk associated with those countries, source of wealth and funds, and information on immediate family members and close associates.[7]

4. *See* Executive Order 13818, "Blocking the Property of Persons Involved in Serious Human Rights Abuse and Corruption," December 21, 2017; *see also* United States Sanctions Human Rights Abusers and Corrupt Actors Across the Globe December 21, 2017.
5. *See* FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) June 2013.
6. *See* FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) June 2013, page 13. FinCEN's regulations similarly include family members and known close associates within the definition of senior foreign political figure. 31 CFR § 1010.605(p).
7. *See* 31 CFR § 1010.620. *See also* FFIEC BSA Examination Manual, "Politically Exposed Persons - Overview," 2015, page 87.

© gettechnical inc 2021

How Corrupt Foreign PEPs and their Facilitators Access the U.S. Financial System

To further assist U.S. financial institutions' effort to insulate themselves from corruption and protect the U.S. financial system from foreign PEP facilitators' illicit use, this advisory highlights a number of typologies used by foreign PEP facilitators to access the U.S. financial system and to obscure and launder the illicit proceeds of high-level political corruption. Appendix 1 provides additional general case studies of financial facilitation methods.

For example, the typologies used by financial facilitators of corrupt PEPs may include the misappropriation of state assets, the use of shell companies, the exploitation of the real estate sector, or any combination of these typologies.

Misappropriation of State Assets

Foreign corrupt PEPs, through their facilitators, may amass fortunes through the misappropriation of state assets and often exploit their own official positions to engage in narcotics trafficking, money laundering, embezzlement of state funds, and other corrupt activities.[8] Such PEPs may exploit corporations, including financial institutions that wish to do business with the government to redirect government resources for their own profit. For example, some PEPs have used offshore leasing companies to sell a commodity such as oil, and do so in a way that benefits particular PEPs (e.g., through the use of shell companies misleadingly named to give the appearance of being related to the government) instead of the government as a whole.[9]

Use of Shell Companies

PEP facilitators commonly use shell companies to obfuscate ownership and mask the true source of the proceeds of corruption. Shell companies are typically non-publicly traded corporations or limited liability companies (LLCs) that have no physical presence beyond a mailing address and generate little to no independent economic value. Shell companies often are formed by individuals and businesses for legitimate purposes, such as to hold stock or assets of another business entity or to facilitate domestic and international currency trades, asset transfers, and corporate mergers. Financial institutions should refer to previously published materials from FinCEN to better understand risks associated with these entities.[10]

8. *See* Treasury Targets Influential Former Venezuelan Official and His Corruption Network May 18, 2018.
9. *See* United States Sanctions Human Rights Abusers and Corrupt Actors Across the Globe December 21, 2017.
10. *See* FinCEN Guidance FIN-2006-G014 "Potential Money Laundering Risks Related to Shell Companies" (November 2006) and SAR Activity Review Issues: Issue 1 (Oct. 2000), Issue 2 (June 2001), and Issue 7 (Aug. 2004).

© gettechnical inc 2021

Corruption in the Real Estate Sector

Real estate transactions and the real estate market have certain characteristics that make them vulnerable to abuse by illicit actors, including corrupt foreign PEPs or PEP facilitators. For example, many real estate transactions involve high-value assets, opaque entities, and processes that can limit transparency because of their complexity and diversity. In addition, the real estate market can be an attractive vehicle for laundering illicit gains because of the manner in which real estate appreciates in value, "cleans" large sums of money in a single transaction, and shields ill-gotten gains from market instability and exchange-rate fluctuations.[11] For these reasons and others, drug traffickers, corrupt officials, and other criminals have used real estate to conceal the existence and origins of their illicit funds.

Red Flags Related to Corrupt Foreign PEPs and their Facilitators

The red flags noted below may help financial institutions identify suspected schemes that corrupt foreign PEPs and their facilitators may use. In applying the red flags below, financial institutions are advised that no single transactional red flag necessarily indicates suspicious activity. Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity and whether the customer exhibits multiple red flags, before determining that a transaction is suspicious. Financial institutions should also perform additional inquiries and investigations where appropriate.

1. Use of third parties when it is not normal business practice.
2. Use of third parties when it appears to shield the identity of a PEP.
3. Use of family members or close associates as legal owners.
4. Use of corporate vehicles (legal entities and legal arrangements) to obscure i) ownership, ii) involved industries, or iii) countries.
5. Declarations of information from PEPs that are inconsistent with other information, such as publicly available asset declarations and published official salaries.
6. The PEP or facilitator seeks to make use of the services of a financial institution or a designated non-financial business or profession (DNFBP)[12] that would normally not cater to foreign or high-value clients.

11. *See* Advisory to Financial Institutions and Real Estate Firms and Professionals August 22, 2017.
12. *See* FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) June 2013. DNFBPs include real estate agents, dealers in precious metals, attorneys, accountants, and company formation agents.

© gettechnical inc 2021

7. The PEP or facilitator repeatedly moves funds to and from countries with which the PEP does not appear to have ties.

8. The PEP or facilitator has a substantial authority over or access to state assets and funds, policies, and operations.

9. The PEP or facilitator has an ownership interest in or otherwise controls the financial institution or DNFBP (either privately or ex officio) that is a counterparty or a correspondent in a transaction.

10. Transactions involving government contracts that are directed to companies that operate in an unrelated line of business (e.g., payments for construction projects directed to textile merchants).

11. Transactions involving government contracts that originate with, or are directed to, entities that are shell corporations, general "trading companies," or companies that appear to lack a general business purpose.

12. Documents corroborating transactions involving government contracts (e.g., invoices) that include charges at substantially higher prices than market rates or that include overly simple documentation or lack traditional details (e.g., valuations for goods and services).

13. Payments involving government contracts that originate from third parties that are not official government entities (e.g., shell companies).

14. Transactions involving property or assets expropriated or otherwise taken over by corrupt regimes, including individual senior foreign officials or their cronies.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Senior Foreign Political Figures and Suspicious Activity Reporting

Consistent with existing regulatory obligations, financial institutions should take reasonable, risk-based steps to identify and limit exposure they may have to funds and other assets associated with individuals and entities involved in laundering illicit proceeds, including the proceeds of foreign corruption. However, financial institutions are reminded that the bulk of PEPs are dedicated public servants and concerns over the criminal and corrupt conduct of some

© gettechnical inc 2021

should not be used as the basis to engage in wholesale or indiscriminate de-risking of any class of customers or financial institutions. FinCEN also reminds financial institutions of previous interagency guidance on providing services to foreign embassies, consulates, and missions.[13]

Due diligence obligations

FinCEN is providing the information in this advisory to assist U.S. financial institutions in meeting their risk-based due diligence obligations to identify individuals providing financial facilitation for, or on behalf of, corrupt PEPs and to not knowingly or wittingly assist such individuals. Financial institutions should establish risk-based controls and procedures that include reasonable steps to ascertain the status of an individual as a foreign PEP and to conduct scrutiny of assets held by such individuals.[14] Financial institutions should assess the risk for laundering of the proceeds of public corruption associated with particular customers, products and services, countries, industries, and transactions.

As of May 11, 2018, FinCEN's Customer Due Diligence (CDD) Rule requires banks; brokers or dealers in securities; mutual funds; and futures commission merchants and introducing brokers in commodities to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[15] Among other things, this should facilitate the identification of legal entities that may be owned or controlled by PEPs.

Enhanced due diligence obligations for private banking accounts

In addition to these general risk-based due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, U.S. financial institutions have regulatory obligations to implement a due diligence program for private banking accounts held for non-U.S. persons that is designed to detect and report any known or suspected money laundering or other suspicious activity.[16] This program must be designed to identify any such

13. *See* Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Embassies, Consulates, and Missions," March 24, 2011 and Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies, and Foreign Political Figures," June 15, 2004.
14. *See* 31 CFR § 1010.620(c) and *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption* (Jan. 16, 2001). *See also* FFIEC BSA Examination Manual, "Politically Exposed Persons - Overview," 2015, pages 290-293.
15. *See* Customer Due Diligence Requirements for Financial Institutions May 11, 2016.
16. *See* 31 CFR § 1010.620(a-b). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition for the term "non-U.S. person" is found in 31 CFR § 1010.605(h).

© gettechnical inc 2021

account owned by, or on behalf of, a senior foreign political figure, and financial institutions are required to apply enhanced scrutiny to such accounts reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.[17]

General obligations for correspondent account due diligence and AML programs

U.S. financial institutions also are reminded to comply with their general due diligence obligations under 31 CFR § 1010.610(a), in addition to their general AML program obligations under 31 U.S.C. § 5318(h) and its implementing regulations.[18] As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their due diligence programs, which address correspondent accounts maintained for foreign financial institutions, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States.

Suspicious activity reporting

A financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, which may include foreign corruption.[19]

Additional SAR reporting guidance on senior foreign political figures

In April 2008, FinCEN issued Guidance to assist financial institutions with reporting suspicious activity regarding proceeds of foreign corruption.[20] A related FinCEN SAR Activity Review, which focused on foreign political corruption, also discusses indicators of transactions that may be related to proceeds of foreign corruption.[21] Financial institutions may find this Guidance and the SAR Activity Review useful in assisting with suspicious activity monitoring and due diligence requirements related to senior foreign political figures.

17. *See* 31 CFR § 1010.620(c).
18. *See* 31 CFR § 1010.210.
19. *See generally* 31 CFR § § 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
20. *See* FinCEN Guidance FIN-2008-G005: "Guidance to Financial Institutions on Filing Suspicious Activity Reports Regarding the Proceeds of Foreign Corruption," April 2008.
21. *See* SAR Activity Review, Issue 19, Focus: Foreign Political Corruption May 2011, particularly pages 29-69.

© gettechnical inc 2021

SAR filing instructions

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. FinCEN further requests that financial institutions select **SAR field 35(l) (Suspected Public/Private Corruption (Foreign)) and reference this advisory by including the key term:**

"Financial Facilitator FIN-2018-A003"

in the SAR narrative and in SAR field 35(z) (Other Suspicious Activity-Other) to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in this advisory.

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying money laundering and other financial crimes associated with foreign and domestic political corruption. SAR reporting is consistently beneficial and critical to FinCEN and U.S. law enforcement analytical and investigative efforts, enforcement of U.S. sanctions, and the overall security and stability of the U.S. financial system.[22]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov. *Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).* The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

22. *See* example case studies in SAR Activity Review, Issue 19, May 2011, beginning on page 25 and Law Enforcement Case Examples.

© gettechnical inc 2021

APPENDIX 1: Case Examples of Financial Facilitation Methods

This appendix includes general case examples which illustrate some of the methods used by financial facilitators.

DRC: Use of Tax Haven Shell Companies by Financial Facilitator of DRC President to Move and Launder Stolen Mining Revenues

On December 20, 2017, the President of the United States included Dan Gertler (Gertler) in the Annex to Executive Order (E.O.) 13818, "Blocking the Property of Persons Involved in Serious Human Rights Abuses and Corruption." In an action simultaneous to E.O. 13818, OFAC designated 19 companies and one individual affiliated with Gertler.[23] Gertler is an international businessman and billionaire who has amassed hundreds of millions of dollars through opaque and corrupt shell company-facilitated mining and oil deals in the Democratic Republic of Congo (DRC), in part, by leveraging his close friendship with DRC President Joseph Kabila. Alongside Gertler's designation, Treasury identified 19 entities owned or controlled by Gertler or his Gibraltar-registered Fleurette Properties Limited (Fleurette), which owns stakes in various Congolese mines through holding companies in offshore tax havens such as the British Virgin Islands (BVI) and the Cayman Islands. Of the companies Treasury designated, six are registered in the BVI and all known addresses correspond to P.O. Box mailing addresses, with multiple companies using the same addresses. Although Gertler does business more publicly through Fleurette, it is the names of these offshore companies that appear on contracts and agreements. The companies appear to have been created for a singular purpose and were rarely disclosed until said agreements had been completed.[24] Between 2010 and 2012 alone, the DRC reportedly lost over $1.36 billion in revenues from the underpricing of mining assets that were sold to offshore companies linked to Gertler. In those instances, Gertler used his close friendship with Kabila to act as an intermediary for mining asset sales in the DRC, requiring some multinational companies to go through Gertler to do business with the Congolese state.[25]

The Gambia, Hizballah, and Iran: Laundering of Stolen Government Funds

On May 17, 2018, OFAC designated Mohammad Ibrahim Bazzi (Bazzi) and Abdallah Safi-Al-Din as Specially Designated Global Terrorists (SDGTs) pursuant to E.O. 13224, which targets terrorists and those providing support to terrorists or acts of terrorism. Bazzi, is a key Hizballah financier who provided Hizballah financial assistance for many years, including millions of

23. *See* Executive Order 13818, "Blocking the Property of Persons Involved in Serious Human Rights Abuse and Corruption," December 20, 2017; *see also* United States Sanctions Human Rights Abusers and Corrupt Actors Across the Globe December 21, 2017.
24. *See* United States Sanctions Human Rights Abusers and Corrupt Actors Across the Globe December 21, 2017.
25. *Ibid.*

© gettechnical inc 2021

dollars generated from his business activities. Bazzi was a close associate of Yahya Jammeh, the former President of The Gambia, whose administration was accused of many human rights abuses, including harsh and potentially life threatening prison conditions; arbitrary arrests; lack of accountability in cases involving violence against women, including rape and female genital mutilation/cutting; trafficking in persons; and child labor.[26] Jammeh personally, or through facilitators (such as Bazzi) acting under his instructions, directed the unlawful withdrawal of at least $50 million of state funds from The Gambia. OFAC also designated that day five companies located in West Africa, Europe, and the Middle East for being owned or controlled by Mohammad Bazzi and another Specially Designated Global Terrorist.[27] According to Treasury, Bazzi operates or transacts in or through Belgium, Lebanon, Iraq, and several countries in West Africa.[28] Bazzi also has business ties to the designated Ayman Joumaa Drug Trafficking and Money Laundering Organization. Between 2009 and 2010, Bazzi also worked with Abdallah Safi-Al-Din, Hizballah's representative to Iran, and the Central Bank of Iran to expand banking access between Iran and Lebanon.[29] Bazzi maintains ties to Hizballah financiers Adham Tabaja and Ali Youssef Charara, who facilitate commercial investments on behalf of Hizballah.[30]

Corruption in South Sudan

On December 21, 2017, the President imposed sanctions on Benjamin Bol Mel (Bol Mel).[31] Bol Mel is the President of ABMC Thai-South Sudan Construction Company Limited (ABMC), and has served as the Chairman of the South Sudan Chamber of Commerce, Industry, and Agriculture.[32] Bol Mel has also served as South Sudanese President Salva Kiir's principal financial advisor, has been Kiir's private secretary, and was perceived within the government as being close to Kiir and the local business community.[33] Several officials were linked to ABMC in spite of a constitutional prohibition on top government officials transacting commercial business or earning income from outside the government.

Bol Mel oversees ABMC, which has been awarded contracts worth tens of millions of dollars by the Government of South Sudan. ABMC allegedly received preferential treatment from high-level officials, and the Government of South Sudan did not hold a competitive process

26. "Annual Country Reports on Human Rights Practices" 2017 (aka the Human Rights Reports), United States Department of State, see background in link, https://www.state.gov/documents/organization/277247.pdf
27. *See* Treasury Targets Key Hizballah Financing Network and Iranian Conduit May 17, 2018.
28. *Ibid.*
29. *See* Treasury Targets Key Hizballah Financing Network and Iranian Conduit May 17, 2018.
30. *See* Treasury Sanctions Hizballah Financier and His Company January 7, 2016.
31. *See* United States Sanctions Human Rights Abusers and Corrupt Actors Across the Globe December 21, 2017.
32. *Ibid.*
33. *Ibid*

© gettechnical inc 2021

for selecting ABMC to do roadwork on several roads in Juba and throughout South Sudan.[34] Although this roadwork had been completed only a few years before, the government budgeted tens of millions of dollars more for maintenance of the same roads.

In September 2017, Treasury took action pursuant to E.O. 13664 in response to the continued deterioration of the humanitarian situation in South Sudan and the role of officials of the South Sudanese Government in undermining the peace, security, and stability of the country.[35] OFAC designated two South Sudanese government officials and one former official for their roles in destabilizing South Sudan and three companies that are owned or controlled by one of the officials. Additionally, FinCEN issued an advisory to financial institutions concerning the potential movement of assets belonging to South Sudanese politically exposed persons.[36]

Laundering of Embezzled Funds by a Former Venezuelan Official and Financial Facilitator

On May 18, 2018, OFAC designated Diosdado Cabello Rondón (Cabello) pursuant to E.O. 13692, for being a current or former official of the Government of Venezuela.[37] Cabello is a former Venezuelan official and is the First Vice-President of the United Socialist Party of Venezuela (PSUV), the political party of Venezuelan President Nicolas Maduro Moros. Cabello is a former army lieutenant who forged a close link at the Venezuelan military academy with former, now-deceased Venezuelan President Hugo Chavez. Cabello has conducted a significant amount of illicit business with others, including Francisco Jose Rangel Gomez (Rangel Gomez), who reported to Cabello. Cabello, Rangel Gomez, and their associates laundered money from the embezzlement of Venezuelan state funds and their dealings with drug traffickers through leasing a series of apartment buildings and commercial shopping centers, and also worked together to illegally access and exploit mines through a subsidiary of a state-owned Venezuelan conglomerate.[38] Although the subsidiary was a legitimate business, Cabello and his associates had front men inside the company who facilitated the illegal extraction and export of natural resources. Venezuelan officials have also used state-owned enterprises to launder money intentionally, to include state-owned enterprises as a cover for drug trafficking and money laundering.

OFAC also designated three other individuals for being current or former officials, or for acting for or on behalf of designated individuals as key figures in Cabello's corruption network including Rafael Alfredo Sarria Diaz, Cabello's front man ("testaferro"), designated for acting for or on behalf of Cabello. Rafael Alfredo Sarria Diaz (Sarria) has laundered

34. *Ibid*
35. Treasury Targets South Sudanese Government Officials and Related Companies for Continued Destabilization September 6, 2017.
36. *See* Advisory on Political Corruption Risks in South Sudan August 22, 2017.
37. *See* Treasury Targets Influential Former Venezuelan Official and His Corruption Network May 18, 2018.
38. *Ibid*

© gettechnical inc 2021

money for Venezuelan officials by buying real estate since 2010.[39] The two have maintained an illicit business relationship since at least 2010, when Sarria and Cabello had partnerships and corporations in Panama, and Sarria owned several real estate properties in Florida that were registered under his own name. In reality, Sarria acted as the named representative for Cabello in the ownership of these properties.[40] As of 2015, Sarria continued to manage multiple properties and financial arrangements for Cabello, and in 2016, he was involved in drug trafficking activities on Cabello's behalf.[41] As of 2018, Sarria advises and assists Cabello, and he profits from the investment of Cabello's corruptly obtained wealth. OFAC has blocked three companies that are owned or controlled by Sarria in Florida: SAI Advisors Inc., Noor Plantation Investments LLC, and 11420 Corp.

Lord's Resistance Army Facilitators Involved in the Illicit Trade of Ivory, Weapons, and Money in Central Africa

On December 13, 2017, OFAC designated Okot Lukwang and Musa Hatari pursuant to E.O. 13667, which targets certain persons contributing to the conflict in the Central African Republic (CAR), including those that support armed groups involved in activities that threaten the peace, security, or stability of the CAR through the illicit trade of natural resources.[42] Both designated persons facilitated the transfer of ivory, weapons, and money in support of the Lord's Resistance Army (LRA).

Lukwang was designated for activities including acting as the LRA's intelligence officer and overseeing supply logistics for Joseph Kony's LRA group, which maintains command and control over three other LRA groups and is composed of his most trusted personnel.[43] Lukwang has coerced civilians to provide him with information on military forces in the area and provided Joseph Kony and other LRA commanders with intelligence reports. Lukwang has also run day-to-day operations of Joseph Kony's LRA group.

In addition, Lukwang acted as the LRA's ivory broker, in charge of selling or trading the LRA's ivory for U.S. dollars, Sudanese pounds, food, weapons, and ammunition, including rocket-propelled grenades and machine gun ammunition.[44] Joseph Kony entrusted Lukwang with the location of hidden tusk caches and used Lukwang and Ali Kony to deal with Darfur-area traders who purchased LRA-trafficked ivory.

39. *Ibid*
40. *Ibid*
41. *Ibid*
42. *See* Treasury Sanctions Lord's Resistance Army Facilitators Involved in the Illicit Trade of Ivory, Weapons, and Money in Central Africa May 18, 2018.
43. *Ibid*
44. *Ibid*

© gettechnical inc 2021

Hatari is the primary supplier of ammunition, mines, weapons, food, supplies, and other goods to the LRA.[45] Hatari, the owner of five shops in the Songo Market in the disputed region of Kafia Kingi, has traded with the LRA since at least 2013.[46] Hatari buys regularly from the LRA, has sold or traded ivory from the LRA at the Songo Market, and has promised to trade anything the LRA wants for ivory.

In May 2015, Lukwang, Ali Kony, and a third LRA commander met with Hatari and other merchants to purchase supplies and plan additional trades.[47] Lukwang translated between the LRA and the merchants to trade ivory for supplies.

Misappropriation of State Assets into Legal Entities Controlled by Facilitators

In 2014, the United States filed a civil forfeiture complaint seeking assets allegedly stolen from the government of Nigeria by dictator, General Sani Abacha (Abacha), and various co-conspirators. The assets are allegedly linked to a scheme to embezzle money from the Nigerian Government during the 1990s and early 2000s through a number of schemes. In one alleged scheme, Abacha and his co-conspirators falsified numerous letters declaring national security emergencies requiring the disbursement of funds by the Central Bank. Through this procedure, the Central Bank disbursed funds worth over $2 billion to Abacha and his associates, who then engaged in a series of complex transactions to transfer those funds to overseas accounts held by legal entities.[48]

Corruption and Residential Real Estate

A high-profile case illustrating money laundering risks in the real estate sector involves Teodoro Nguema Obiang Mangue, (Obiang) the Vice President of Equatorial Guinea, in which the U.S. Department of Justice filed a forfeiture complaint seeking forfeiture of over $68 million in assets—including a $30 million Malibu estate—associated with funds allegedly misappropriated from the Equatoguinean government. In laundering these funds in or through the United States from in or about 2006 through 2010, Obiang used several U.S. nominees to open shell accounts and banks accounts on his behalf while concealing from U.S. banks his ownership, control and association with these funds. The nominees identified included lawyers, and other employees of his. The assets purchased using the proceeds of this scheme included a 10-acre estate in Beverly Hills, a $38 million jet aircraft, a Ferrari and several items of Michael Jackson memorabilia.[49]

45. *Ibid*
46. *Ibid*
47. *Ibid*
48. *See* United States v. All Assets Held in Account Number 80020796, in the Name of Doraville Props. Corp., Case No. 1:13-cv-01832 (D.D.C. Nov.18, 2013).
49. *See* One Michael Jackson Signed Thriller Jacket, et al., No. CV-13-9169-GW-SS (C.D. Cal. Oct. 10, 2014).

© gettechnical inc 2021

FinCEN's analysis of Bank Secrecy Act (BSA) and other data, particularly data gathered through the use of FinCEN's recent Geographic Targeting Orders requiring the collection of beneficial ownership information of companies purchasing real estate in a number of markets in the United States, indicates that high-value residential real estate markets are vulnerable to misuse by foreign and domestic criminal organizations and corrupt actors, especially those misusing otherwise legitimate limited liability companies or other legal entities to shield their identities.[50] In addition, when these transactions are conducted without any financing (e.g., "all-cash"), they mostly avoid traditional anti-money laundering measures adopted by lending financial institutions, presenting increased risk.

Iran: Treasury Targets Human Rights Abuses, Censorship, and Enhanced Monitoring by the Iranian Government

On May 30, 2018, OFAC designated Ansar-e Hizballah pursuant to E.O. 13553 for being an official of the Government of Iran or a person acting on behalf of the Government of Iran (including members of paramilitary organizations) who is responsible for or complicit in, or responsible for ordering, controlling, or otherwise directing, the commission of serious human rights abuses against persons in Iran or Iranian citizens or residents, or the family members of the foregoing.[51] Ansar-e Hizballah is an organization supported by the Iranian regime that is responsible for ordering, controlling, or otherwise directing, serious human rights abuses against the Iranian people. Ansar-e Hizballah has been involved in the violent suppression of Iranian citizens and has collaborated with the Basij Resistance Force to attack Iranian students with knives, tear gas, and electric batons. In addition, the U.S. Government has linked Ansar-e Hizballah to acid attacks against women in the city of Isfahan. Multiple women who were not dressed in accordance with the regime's standards had acid thrown at them, severely injuring them and creating a climate of fear. Abdolhamid Mohtasham, a founding member and key leader of the group, plays a significant role in overseeing the group's actions. He has threatened to use Ansar-e Hizballah to patrol Iranian streets and attack women whom he deems to be unvirtuous. Additionally, OFAC designated Hanista Programing Group, an entity that has operated information or communications technology that facilitates monitoring or tracking that could assist or enable serious human rights abuses by or on behalf of the Government of Iran. Hanista Programing Group is responsible for creating and distributing alternative versions of the popular messaging and social media application Telegram that facilitate the Iranian regime's monitoring and tracking of Iranian and international users. This monitoring and tracking functionality could assist or enable serious human rights abuses by the Government of Iran.

50. *See* Advisory to Financial Institutions and Real Estate Firms and Professionals August 22, 2017.
51. *See* Treasury Targets Key Hizballah Financing Network and Iranian Conduit May 17, 2018.

© gettechnical inc 2021

FinCEN FIN-2018-A001: Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (North Korea Information only) (2/9/2018)

UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

ADVISORY

FIN-2018-A001 February 9, 2018

Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies

On November 3, 2017, the Financial Action Task Force (FATF) updated its list of jurisdictions with strategic anti-money laundering and combatting the financing of terrorism (AML/CFT) deficiencies. The changes may affect U.S. financial institutions' obligations and risk-based approaches with respect to relevant jurisdictions.

As part of the FATF's listing and monitoring process to ensure compliance with its international AML/CFT standards, the FATF identifies certain jurisdictions as having strategic deficiencies in their AML/CFT regimes.[1] These jurisdictions appear in two documents: (1) the "FATF Public Statement," which includes jurisdictions that are subject to the FATF's call for countermeasures or are subject to enhanced due diligence (EDD) due to their strategic AML/CFT deficiencies, and (2) "Improving Global AML/CFT Compliance: On-going Process," which includes jurisdictions identified by the FATF as having strategic AML/CFT deficiencies.[2] On November 3, 2017, the FATF updated both documents with the concurrence of the United States. Financial institutions should consider these changes when reviewing their obligations and risk-based policies, procedures, and practices with respect to the jurisdictions noted below.[3]

FATF "Public Statement":

- Democratic People's Republic of Korea (DPRK) and Iran

FATF "Improving Global AML/CFT Compliance: On-going Process":

- Remaining on list: Bosnia and Herzegovina, Ethiopia, Iraq, Syria, Vanuatu, and Yemen
- Added to list: Sri Lanka, Trinidad and Tobago, Tunisia,
- Removed from list: Uganda

1. The FATF (www.fatf-gafi.org) is a 37-member intergovernmental body that establishes international standards to combat money laundering and counter the financing of terrorism and proliferation of weapons of mass destruction. The United States is a member of the FATF.
2. The FATF public identification of countries with strategic AML/CFT deficiencies is in response to the G-20 leaders' call for the FATF to reinvigorate its process for assessing countries' compliance with international AML/CFT standards. The G-20 leaders have consistently called for the FATF to issue regular updates on jurisdictions with strategic deficiencies. Specifically, within the FATF, the International Cooperation Review Group (ICRG) monitors and identifies countries with AML/CFT deficiencies. For more information on the ICRG procedures, please visit the FATF's website – www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/moreabouttheinternationalco-operationreviewgroupicrg.html.
3. *See* 31 U.S.C. § 5318(h) and (i).

© gettechnical inc 2021

I. Jurisdictions that are subject to the FATF's call for countermeasures or are subject to EDD due to their strategic AML/CFT deficiencies

The FATF has stated that the following jurisdictions have strategic deficiencies in their AML/CFT regimes and has called upon its members and urged all jurisdictions to (1) impose countermeasures and/or (2) consider the risk arising from each jurisdiction due to a lack of sufficient progress in addressing AML/CFT deficiencies.

Please click on each jurisdiction for additional information.

A. Countermeasures:

Democratic People's Republic of Korea (DPRK)

B. Enhanced Due Diligence:

Iran

Summary of Changes to this List

- DPRK: No changes.

The FATF remains concerned with the threat posed by illicit activities related to the proliferation of weapons of mass destruction (WMDs) and its financing emanating from the DPRK. Further, the FATF remains concerned with the DPRK's failure to address the significant deficiencies in its anti-money laundering and combating the financing of terrorism (AML/CFT) regime and the serious threats they pose to the integrity of the international financial system. In addition to enhanced scrutiny, the FATF further calls on its members and urges all jurisdictions to apply effective countermeasures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions (UNSCRs), to protect their financial sectors from money laundering, financing of terrorism, and WMD proliferation financing risks emanating from the DPRK. Jurisdictions should take necessary measures to close existing branches, subsidiaries, and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks, where required by relevant UNSCRs.

See the full FATF statements on DPRK: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/statement-dprk-nov-2017.html and http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-november-2017.html

- Iran: No changes.

See the full FATF statements on Iran: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-november-2017.html and http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-november-2017.html

© gettechnical inc 2021

Review of Guidance Regarding DPRK and Iran

Democratic People's Republic of Korea (DPRK)

The FATF calls on its members and other countries to apply countermeasures against the DPRK to protect the international financial system from money laundering and terrorist financing risks. The FATF Public Statement on the DPRK continues to reflect the high risk of proliferation finance attributable to the DPRK, consistent with UNSCRs 2397, 2375, 2371, 2270, and 2321. In particular, the FATF reaffirmed its call that jurisdictions terminate correspondent relationships with DPRK banks, where required by relevant UNSCRs. Financial institutions should be acutely aware of the financial provisions and prohibitions contained in the UNSCRs against the DPRK.[4]

In addition to UN sanctions, Treasury's Office of Foreign Assets Control (OFAC) maintains a robust sanctions program on North Korea through the North Korea Sanctions Regulations and Executive Orders (E.O.) 13382, 13466, 13551, 13570, 13687, 13722, and 13810.[5] Collectively, these sanctions prohibit U.S. persons, including U.S. financial institutions, from engaging in nearly all transactions involving the DPRK.[6] These sanctions are a direct response to North Korea's ongoing development of weapons of mass destruction (WMD) and their means of delivery in continued violation of the UNSCRs.

U.S. financial institutions should be particularly aware of the extensive nature of the sanctions associated with E.O. 13810 (September 2017).[7] Section 4 of E.O. 13810 allows OFAC to impose measures on foreign financial institutions that, on or after the date of the E.O., knowingly conduct or facilitate any significant transaction on behalf of a North Korea-related blocked person or knowingly conduct or facilitate any significant transaction in connection with trade with North Korea. The sanctions imposed since E.O. 13810 was issued have included actions against companies and individuals involved in shipping and transportation (including specific vessels), trading companies, financial representation, and banking.

4. Relevant UNSCRs include 2397 (December 2017), 2375 (September 2017), 2371 (August 2017), 2356 (June 2017), 2321 (November 2016), 2270 (March 2016), 2094 (March 2013), 2087 (January 2013), 1874 (June 2009), and 1718 (October 2006). *See* http://www.un.org/en/sc/documents/resolutions/ for more information.

5. *See* https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx.

6. Further information about these sanctions is available on OFAC's Resource Center for DPRK Sanctions and the OFAC Recent Actions web page. OFAC most recently took new sanctions action related to DPRK, pursuant to Executive Orders 13687 and 13810 on January 24, 2018. OFAC previously took sanctions actions related to DPRK on December 26, 2017, pursuant to Executive Order 13687; on November 21, 2017, pursuant to Executive Orders 13810 and 13722; on October 26, 2017, pursuant to Executive Order 13687 and 13722; on September 26, 2017, pursuant to Executive Order 13810; and on August 22, 2017, pursuant to Executive Orders 13382 and 13722. OFAC took other DPRK-related sanctions pursuant to one or more of these same authorities on June 29, 2017, June 1, 2017, March 31, 2017, December 2, 2016, and September 26, 2016. On November 20, 2017, the United States designated DPRK a state sponsor of terrorism, see https://www.state.gov/j/ct/list/c14151.htm.

7. *See* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170921.aspx and https://www.treasury.gov/press-center/press-releases/Pages/sm0162.aspx.

© gettechnical inc 2021

Other Treasury actions underscore the serious risks that any financial activity involving the DPRK may facilitate WMD and ballistic missile activities. On November 4, 2016, Treasury issued a final rule, effective December 9, 2016, imposing the fifth special measure against the DPRK, consistent with the associated notice of finding that the DPRK is a jurisdiction of "primary money laundering concern" under Section 311 of the USA PATRIOT Act.[8] The finding and rule stressed that the North Korean government continues to use state-controlled financial institutions and front companies to surreptitiously conduct illicit international financial transactions, some of which support the proliferation of weapons of mass destruction and the development of ballistic missiles. The final rule prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, North Korean banking institutions and requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against the use of such accounts to process transactions involving North Korean financial institutions.

On November 2, 2017, Treasury issued a final rule, effective December 8, 2017, under Section 311 of the USA PATRIOT Act that severs Bank of Dandong, a Chinese bank that acts as a conduit for illicit North Korean financial activity, from the U.S. financial system. The final action stressed that the Bank of Dandong acts as a conduit for North Korea to access the U.S. and international financial systems, including by facilitating millions of dollars of transactions for companies involved in North Korea's WMD and ballistic missile programs. Bank of Dandong also facilitates financial activity for North Korean entities designated by the United States and listed by the UN for proliferation of WMDs, as well as for front companies acting on their behalf. The final rule: a) prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, the Bank of Dandong; b) requires covered financial institutions to take reasonable steps not to process a transaction for the correspondent account of a foreign bank in the United States if such a transaction involves the Bank of Dandong; and c) requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving Bank of Dandong.[9]

The Financial Crimes Enforcement Network (FinCEN) also issued an advisory in tandem with the Bank of Dandong Section 311 Final Rule to further alert financial institutions to schemes commonly used by North Korea to evade U.S. and United Nations (UN) sanctions, launder funds, and finance the North Korean regime's weapons programs.[10]

---

8. *See* https://www.treasury.gov/press-center/press-releases/Pages/jl0603.aspx and https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf [81 FR 78715 (November 9, 2016)]. FinCEN issued the finding and notice of proposed rulemaking (NPRM) on June 1, 2016 [81 FR 35441 (June 2, 2016) and 81 FR 35665 (June 3, 2016)], respectively; *see* https://www.fincen.gov/sites/default/files/shared/2016-13038(DPRK_Finding).pdf and https://www.fincen.gov/sites/default/files/shared/2016-13037(DPRK_NPRM).pdf.

9. *See* https://www.treasury.gov/press-center/press-releases/Pages/sm0205.aspx, https://www.treasury.gov/press-center/press-releases/Pages/jl0603.aspx, and https://www.fincen.gov/sites/default/files/federal_register_notices/2017-11-02/Bank%20of%20Dandong%20311%20Final%20Rule.pdf [31 CFR Part 1010].

10. *See* FinCEN Advisories pertaining to the DPRK: FIN-2017-A008 (November 2, 2017), FIN-2013-A005, FIN-2009-A002, and FinCEN Advisory – Issue 40.

© gettechnical inc 2021

Iran

Not included herewith

© gettechnical inc 2021

Review of Guidance on Section 312 Obligations to the DPRK and Iran

FinCEN advises U.S. financial institutions to apply enhanced due diligence when maintaining correspondent accounts for foreign banks operating under a banking license issued by a designated country.[14] Financial institutions must also comply with the extensive U.S. restrictions and prohibitions against opening or maintaining any correspondent accounts, directly or indirectly, with foreign banks licensed by the DPRK or Iran.

As required by the regulations implementing the Bank Secrecy Act, covered financial institutions should ensure that their enhanced due diligence programs include, at a minimum, steps to:

- Conduct enhanced scrutiny of correspondent accounts to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable law and regulation;
- Determine whether the foreign bank for which the correspondent account is established or maintained in turn maintains correspondent accounts for other foreign banks that use the foreign correspondent account established or maintained by the covered financial institution and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks; and
- Determine, for any correspondent account established or maintained for a foreign bank whose shares are not publicly traded, the identity of each owner of the foreign bank and the nature and extent of each owner's ownership interest.[15]

II. Jurisdictions identified by the FATF as having strategic AML/CFT deficiencies

The FATF publicly identifies jurisdictions with strategic AML/CFT regime deficiencies for which the jurisdictions have developed an action plan with the FATF. Consequently, these jurisdictions are included in the following list of jurisdictions with strategic AML/CFT deficiencies, as described in the FATF's "Improving Global AML/CFT Compliance: On-going Process".

14. *See* 31 U.S.C. § 5318(i); 31 CFR § 1010.610(b) and (c) (Enhanced Due Diligence obligations for correspondent accounts established, maintained, administered or managed in the United States for foreign banks). The obligations under Section 312 of the USA PATRIOT Act are consistent with FATF's statements on the DPRK and Iran.

15. *See* 31 CFR § 1010.610(b): Enhanced Due Diligence for correspondent accounts established, maintained, administered or managed in the United States for foreign banks.

[pages 7 & 8 intentionally excluded]

© gettechnical inc 2021

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov,. *Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).* The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

© gettechnical inc 2021

FinCEN FIN-2017-A008: Advisory on North Korea's Use of the International Financial System (11/2/2017)

UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

ADVISORY

FIN-2017-A008 November 2, 2017

Advisory on North Korea's Use of the International Financial System

North Korea uses front and trade companies to disguise, move, and launder funds to finance its nuclear and ballistic missile programs.

This Advisory should be shared with:

- *Chief Risk Officers*
- *Chief Compliance Officers*
- *Legal Departments*
- *AML/BSA Departments*
- *AML/BSA Analysts*
- *Sanctions Analysts*

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to further alert financial institutions to North Korean schemes being used to evade U.S. and United Nations (UN) sanctions, launder funds, and finance the North Korean regime's weapons of mass destruction (WMD) and ballistic missile programs. This advisory is being issued in tandem with the final rule issued by FinCEN under Section 311 of the USA PATRIOT Act prohibiting U.S. financial institutions from opening or maintaining a correspondent account for, or on behalf of, Bank of Dandong, and as a follow up to the September 26, 2017, designations by Treasury's Office of Foreign Assets Control (OFAC), which targeted several representatives of designated North Korean financial institutions.[1] This advisory provides financial red flags of illicit North Korean schemes, including the use of financial representatives world-wide. It also highlights the use of China-based front or shell companies, trading companies, and financial institutions operating in areas bordering the Democratic People's Republic of Korea (DPRK). These red flags will assist financial institutions in identifying and reporting suspected illicit activity by the North Korean government and its financial institutions.

Recent Treasury Actions

The U.S. Department of the Treasury is implementing a strategy designed to impose maximum pressure on the DPRK and to protect the U.S. and international financial systems from misuse by the DPRK. The Treasury Department continues to take actions targeting the DPRK's ongoing development of its WMD and ballistic missile programs, as well as its continued violations of UN Security Council resolutions (UNSCRs).[2] Recent Treasury Department actions include the following:

1. *See* https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures for more information on today's FinCEN Section 311 final rule related to the Bank of Dandong. For more information on the most recent OFAC sanctions, *see* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170926_33.aspx.
2. Relevant UNSCRs include 2375 (September 2017), 2371 (August 2017), 2356 (June 2017), 2321 (November 2016), 2270 (March 2016), 2094 (March 2013), 2087 (January 2013), 1874 (June 2009), and 1718 (October 2006). *See* http://www.un.org/en/sc/documents/resolutions/ for more information.

© gettechnical inc 2021

- OFAC has issued a number of DPRK-related designations and identifications, including pursuant to the new Executive Order 13810, which was announced on September 21, 2017. This executive order significantly expands Treasury's authorities to target persons who continue to finance and facilitate North Korea's economic activity. The OFAC designations and identifications, to include over 250 persons to date, expose the North Korean regime's international reach and continued access to the international financial system;[3]
- FinCEN has designated the DPRK as a jurisdiction of primary money laundering concern subject to special countermeasures under Section 311 of the USA PATRIOT Act to safeguard the U.S. financial system;[4]
- In tandem with this advisory, FinCEN has issued a final rule that prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, Bank of Dandong.[5] FinCEN found Bank of Dandong to be of "primary money laundering concern" for serving as a gateway for North Korea to access the U.S. and international financial systems despite U.S. and UN sanctions. Covered financial institutions are also required to apply special due diligence measures to their foreign correspondent accounts reasonably designed to guard against such accounts being used to process transactions involving the Bank of Dandong; and
- FinCEN has issued advisories and guidance about the increased risk that the DPRK and North Korean entities pose to U.S. and foreign financial institutions.[6]

3. OFAC's sanctions prohibit U.S. persons, including U.S. financial institutions, from engaging in most transactions involving the DPRK, the Government of North Korea, and the Korean Workers' Party. In addition to OFAC's actions on September 26, 2017, OFAC recently imposed DPRK-related sanctions actions pursuant to Executive Orders 13382 and 13722 on August 22, 2017. OFAC imposed DPRK-related sanctions pursuant to those same authorities on June 29, 2017. *See* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170629.aspx for more information. OFAC also imposed DPRK-related sanctions actions pursuant to those same Executive Orders and/or Executive Order 13687 on June 1, 2017, March 31, 2017, December 2, 2016, and September 26, 2016. For the complete listing of all OFAC actions related to the DPRK, *see* https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx.
4. FinCEN's Section 311 rule imposing the fifth special measure against the DPRK: a) prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, North Korean banking institutions; b) requires covered financial institutions to take reasonable steps not to process a transaction for the correspondent account of a foreign bank in the United States if such a transaction involves a North Korean financial institution; and c) requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving North Korean financial institutions. *See* https://www.treasury.gov/press-center/press-releases/Pages/jl0603.aspx and https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf [81 FR 78715 (November 9, 2016)] as codified in 31 CFR § 1010.659. FinCEN issued the finding and initial notice of proposed rulemaking (NPRM) on June 1, 2016 [81 FR 35441 (June 2, 2016) and 81 FR 35665 (June 3, 2016)], respectively; *see* https://www.fincen.gov/sites/default/files/shared/2016-13038(DPRK_Finding).pdf and https://www.fincen.gov/sites/default/files/shared/2016-13037(DPRK_NPRM).pdf. FinCEN issued the final rule on November 2, 2017: *see* https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures.
5. In July 2017, FinCEN issued a Notice of Proposed Rulemaking (NPRM) finding the China-based Bank of Dandong to be a "foreign financial institution of primary money laundering concern" under Section 311 of the USA PATRIOT Act. *See* 82 FR 31537 (July 2017) and "Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern" (July 2017).
6. *See* FinCEN Advisories pertaining to the DPRK: FIN-2013-A005 (July 2013), FIN-2009-A002 (June 2009), and FinCEN Advisory – Issue 40 (December 2005). *See also* FIN-2017-A005 (September 2017) regarding the June 23, 2017, Financial Action Task Force (FATF) "Public Statement" on the DPRK.

© gettechnical inc 2021

How North Korea Accesses the International Financial System

Although international sanctions have significantly isolated North Korean banks, the North Korean government continues to use state-owned entities and banks, as well as bulk-cash smuggling and trade, to access the international financial system. Such access occurs through aliases, agents, and individuals in strategic jurisdictions, as well as through long-standing networks of front or shell companies and embassy personnel.[7] North Korea's illicit financial activity supports, among other things, its proliferation of WMD-related technology and missile systems as well as conventional weapons programs.

As explained in the February 2016 United Nations Security Council "Report of the Panel of Experts established pursuant to resolution 1874" (hereafter referred to as "UN Report"), the North Korean government uses state-owned entities and banks to conduct transactions in support of its WMD and ballistic missile programs. These North Korean state-owned enterprises in turn use foreign-based front or shell companies and covert representatives based abroad to obfuscate the true originator, beneficiary, and purpose of transactions, enabling millions of dollars of North Korean illicit financial activity to flow through U.S. correspondent accounts.

To conduct these transactions, the UN Report notes that North Korean state-owned enterprises typically orchestrate elaborate trade-based payment schemes. For instance:

(1) Sale/Export of Natural Resources: The DPRK sells/exports natural resources (*e.g.*, coal, iron ore, and minerals) to China-based companies, often located near the North Korean border, such as in Liaoning province.[8] The Chinese companies, in turn, sell such natural resources to the Asian market.

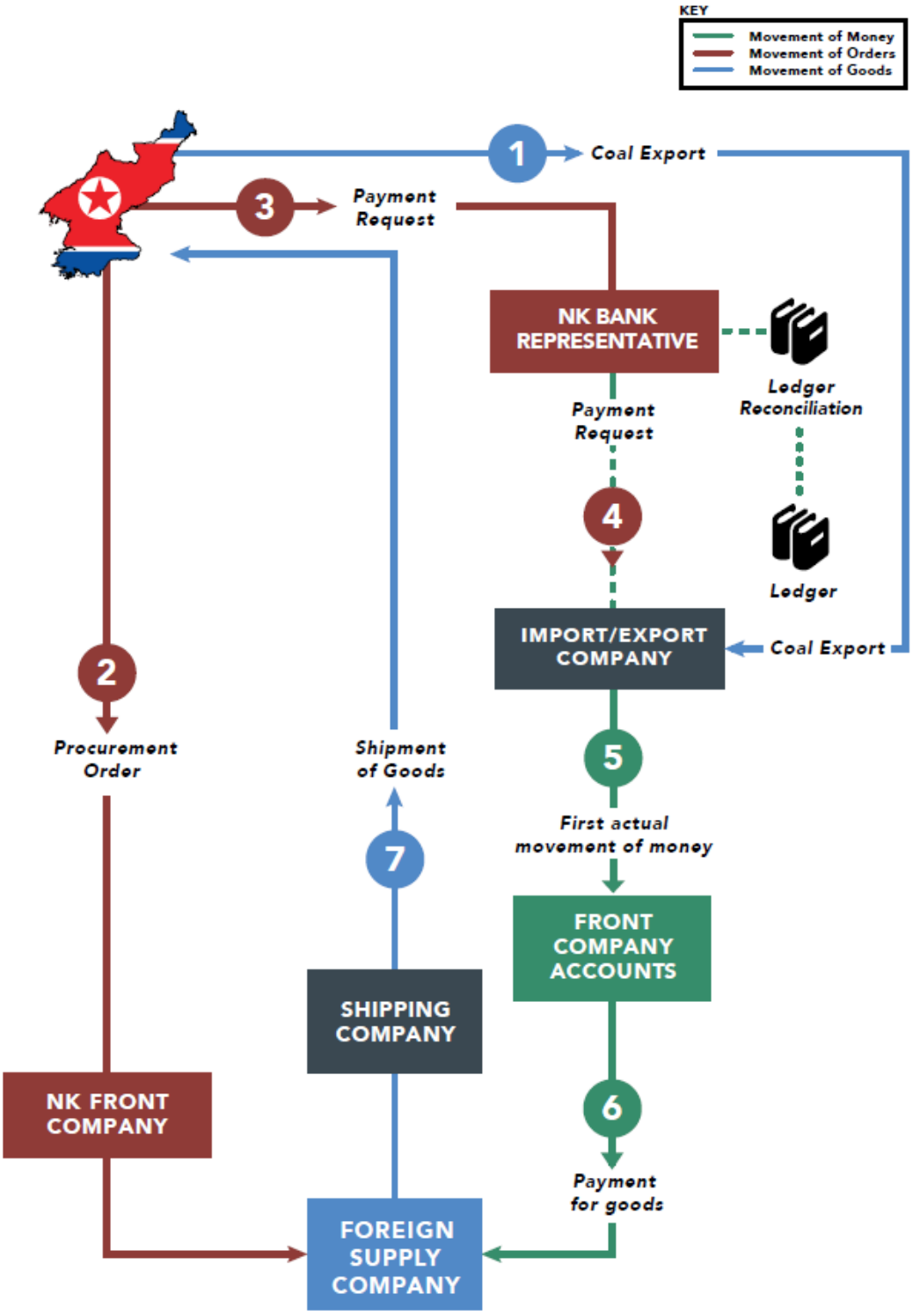
(2) Indirect Payment for Natural Resources: Rather than directly paying the DPRK, the China-based companies divide their payments into smaller outflows in a complex layering scheme directed to front companies, shell companies, shipping or trade businesses based in Asia (often registered in Hong Kong), and other companies based in various offshore jurisdictions (*e.g.*, British Virgin Islands, Marshall Islands, and the Seychelles). Various financial representatives and corporate service providers may establish the front or shell companies or serve as representatives of the various involved entities.

(3) Import/Smuggling of Goods: The front or shell companies then use the received payments to purchase and ship commodities to the DPRK. These commodity shipments in turn may be used to smuggle goods that the North Korean government uses to build its WMD and ballistic missile programs (see below graphic).

7. *See* United Nations Security Council "Report of the Panel of Experts established pursuant to resolution 1874" (February 2016).

8. UNSCR 2371 prohibits imports of North Korean coal, iron and iron ore, lead and lead ore, and seafood. UNSCR 2375 prohibits imports of textiles, among other new measures.

© gettechnical inc 2021



4

© gettechnical inc 2021

These types of trade-based schemes allow the North Korean government to evade U.S. and UN sanctions by directing payments for natural resource sales to its front and shell companies. The North Korean government can then use these laundered proceeds, through its front and shell companies, to access the international financial system and acquire technology for use in its WMD and ballistic missile programs. North Korean representatives often use these companies to establish bank accounts at local banks and take orders from sanctioned North Korean entities.

Treasury believes that the DPRK uses and maintains a network of financial representatives, primarily in China, who operate as agents for North Korean financial institutions. In this capacity, these representatives orchestrate schemes, set up front or shell companies, and manage surreptitious bank accounts to move and disguise illicit funds, evade sanctions, and finance the proliferation of the DPRK's WMD and ballistic missile programs.

For example, on August 22, 2017, and on September 26, 2017, OFAC designated Mingzheng International Trading Limited (Mingzheng), a China- and Hong Kong-based front company, additional persons, several dozen North Korean individuals, as well as a number of banks, for their involvement in evading sanctions and laundering funds on behalf of the North Korean regime. Treasury believes that the bank accounts used by these sanctioned persons are maintained predominantly at major Chinese financial institutions. These sanctioned North Korean persons have used their accounts to access the U.S. and international financial systems in support of the DPRK's WMD and ballistic missile and conventional weapons programs.

U.S. Forfeiture Actions Reveal Complex North Korean Schemes to Evade Sanctions

Recent actions by the Department of Justice also highlight the DPRK's methods to evade sanctions:

Mingzheng International Trading Limited (Mingzheng). On June 14, 2017, the U.S. Department of Justice (DOJ) initiated a forfeiture action against Mingzheng International Trading Limited (Mingzheng), for allegedly operating as a Hong Kong-based front company for a foreign-based branch of the North Korea-based Foreign Trade Bank (FTB).[9] The forfeiture complaint illustrates how the DPRK allegedly used a network of front companies and corporate representatives to evade U.S. sanctions by acting on behalf of a designated North Korean bank. According to the forfeiture complaint, "North Korea has used the state-run Foreign Trade Bank ("FTB") to work with a host of front companies in order to access the U.S. financial system and evade the U.S. sanctions imposed on FTB and its sanctioned affiliates,"[10] and "Mingzheng acts as a front company to make U.S. dollar payments on behalf of a covert foreign branch of FTB, which is otherwise barred from making such U.S. dollar payments." According to the

9. *See* "United States Files Complaint to Forfeit More Than $1.9 Million From China-Based Company Accused of Acting as a Front for Sanctioned North Korean Bank" (June 2017).

10. At the time of this forfeiture action, Foreign Trade Bank was a U.S. designated entity; *see* https://www.treasury.gov/press-center/press-releases/Pages/jl1876.aspx.

© gettechnical inc 2021

complaint, Mingzheng has no website, stated no business purpose in corporate documents, made payments for products in unrelated industries, and served as a counterparty to multiple wire transfers over a short period of time. In this case, Mingzheng allegedly conducted 20 wire transfers in U.S. dollars, totaling about $1.9 million, between October and November 2015.

Velmur Management Pte Ltd (Velmur) and Transatlantic Partners Pte. Ltd (TransAtlantic); Dandong Chengtai Trading Co. Ltd, also known as Dandong Zhicheng Metallic Material Co., Ltd (Dandong Zhicheng). On August 22, 2017, in conjunction with OFAC's DPRK-related sanctions, the DOJ initiated similar forfeiture actions involving more than $11 million against 1) Velmur, a Singapore-based company, and TransAtlantic and 2) Dandong Zhicheng, a company in Dandong, China.[11] The forfeiture complaints allege, "(T)he companies have participated in schemes to launder U.S. dollars on behalf of sanctioned North Korean entities….(and) the companies participated in financial transactions in violation of the International Emergency Economic Powers Act (IEEPA), the North Korean Sanctions and Policy Enhancement Act of 2016, and federal conspiracy and money laundering statutes." In the case of Velmur and TransAtlantic, the companies acted as fronts for designated North Korean banks to facilitate U.S. dollar payments to an OFAC-sanctioned Russian oil products supplier involved in the shipping oil and other petroleum products to the DPRK. The Dandong Zhicheng complaint also involved the facilitation of U.S. dollar payments to benefit a U.S.-designated entity, the North Korean Workers Party, through the purchase of Chinese coal.

Red Flags of Potential North Korean Illicit Financial Activity

Many North Korean-related front companies, financial representatives, and corporate service providers working on behalf of the North Korean government often share similar characteristics. While none of these characteristics are *per se* indicative of North Korean involvement, financial institutions may consider treating these characteristics as red flags to ensure that a financial institution's correspondent accounts are not being utilized by entities or other financial facilitators on behalf of North Korean financial institutions and the DPRK. These red flags also will assist financial institutions in identifying potentially suspicious transactions that are required to be reported promptly to FinCEN.

- **Geography**: As illustrated above, many North Korean front or shell companies, banking and financial representatives, and corporate service providers used by the North Korean government are based in China and/or use Chinese banks to facilitate the movement of illicit funds on behalf of the North Korean government.

11. *See* "United States Files Complaints to Forfeit More Than $11 Million From Companies That Allegedly Laundered Funds To Benefit Sanctioned North Korean Entities" (August 2017) (noting that "the complaints are the first filed actions based on the 2016 North Korea Sanction and Policy Enhancement Act.") For information on the OFAC designation of IPC, *see* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170601.aspx.

© gettechnical inc 2021

- *Financial Representatives Areas of Activity*: These representatives are typically North Korean-born and often use Chinese aliases or Chinese facilitators to establish and operate bank accounts and front or shell companies, particularly in Liaoning province and the Hong Kong Special Administration Region. Each representative may appear as a corporate officer of multiple, seemingly unrelated, front or shell companies that also often transact with each other. North Korean representatives may also appear as authorized signers for accounts maintained by the front or shell companies.

- *Corporate Registration and Shared Business Addresses*: Based on information from the UN Report and other information available to Treasury, a number of front and shell companies operating on behalf of the North Korean government are registered in either Liaoning province, China—specifically in the municipalities of Dalian, Dandong, Jinzhou, and Shenyang—which borders the DPRK, or in Hong Kong, a major financial center with a variety of corporate service providers. Additionally, front and shell company addresses are frequently recycled and used for multiple business registrations. A key example of this is the Jiadi Square area in the city of Dandong, Liaoning province. The OFAC-sanctioned corporation Dandong Hongxiang Industrial Development Co. Ltd, and several suspected (and possibly related) shell companies, maintained Jiadi Square addresses, which is also home to North Korea's Dandong-based consulate.

- *Liaoning-Based Banking*: The proximity of the Chinese province of Liaoning to the North Korean border makes it an attractive location for North Korean illicit actors to access the international financial system. FinCEN has observed North Korean-related financing involving correspondent account transactions conducted by, or on behalf of, Liaoning-based banks, including, but not limited to, institutions located in the cities of Dalian, Dandong, Jinzhou, and Shenyang. For example, FinCEN finalized its Section 311 rulemaking against Bank of Dandong, which is located in Liaoning province. FinCEN found that Bank of Dandong acts as a conduit for North Korea to access the U.S. and international financial systems, including by facilitating millions of dollars of transactions for companies involved in North Korea's WMD and ballistic missile programs.[12]

12. *See* Footnote 5.

© gettechnical inc 2021

Surge Activity Cycles: North Korean representatives use and deposit funds through seemingly unrelated companies that share the same address. These companies are usually "cycled," or used for a short period of time before being retired. However, associated bank accounts may stay open during lengthy periods of inactivity. Financial activity transacted through these companies can often occur in cycles, whereby one company (Company A) will pay a common beneficiary for a period of time and then cease payments. Once Company A ceases making payments, a different company (Company B, which shares an address with Company A), pays the same beneficiary. Reviewing the timing of transactions and associated payees may allow financial institutions to determine whether seemingly unrelated companies are being utilized for this type of financial cycling.

Common Front Companies and Supporting Indicators: FinCEN has identified that shipping and import/export businesses are often employed as fronts for illicit North Korean activity. Law enforcement information available to FinCEN has identified that textile, garment, fishery, and seafood businesses are also frequently listed as the business lines for various front companies. The UN Report also highlighted the North Korean government's reliance on coal exports to access foreign currency. Other potential related indicators include:

- *Companies Sharing Owners or Managers, Phones, or Employees*: DPRK-linked financial facilitators often establish and use multiple companies with the same owners or managers. These companies also frequently share addresses, telephone numbers, and employees, and they may transact with similar business partners. The use of multiple companies provides financial facilitators with alternatives in the event that one company is compromised. Multiple companies also allow financial facilitators to divert attention from any particular company, avoiding scrutiny, and increasing their ability to launder money. The Department of Justice's complaint against U.S.-designated Mingzheng highlighted an example of companies sharing managers and employees. In addition, Luo Chuanxu, a U.S.-designated Chinese national, allegedly established multiple front companies to facilitate payments on behalf of UN- and U.S.-designated Korea Kwangsong Banking Corporation (KKBC). Luo allegedly facilitated numerous payments for both Dandong Hongxiang Industrial Development Company Ltd (DHID), which was designated by OFAC in September 2016, and Mingzheng.[13]

- *Substantial Financial Activity Unrelated to Stated Areas of Business*: North Korean front companies often lack a stated business purpose, and the payments they receive for products and services are unrelated to an entity's specified lines of business. For example, as noted in the UN Report and highlighted in the DOJ complaint against Dandong Zhicheng, one company (Company A) imports coal from the DPRK—without prepaying for it—and resells it to coal customers around the world. Company A then retains the proceeds of these U.S. dollar sales, including the money owed to the DPRK. The DPRK

13. *See* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20160926.aspx and https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170822.aspx, respectively.

© gettechnical inc 2021

subsequently sends payment instructions to Company A for items the regime would like to purchase. Company A then uses the retained proceeds to purchase the items for export to the DPRK. The items are typically in unrelated industries, such as bulk commodities (sugar, rubber, petroleum products, soybean oil), cell phones, luxury items, or dual-use technology.

- *Lack of Online Presence*: Businesses serving as front companies for illicit North Korean activity frequently do not maintain a website or other online presence despite their significant transactions.

Regulatory Obligations for U.S. Financial Institutions

Prohibition on Use of Correspondent Accounts involving North Korean Financial Institutions

FinCEN's November 2016 Section 311 action against the DPRK and November 2017 Section 311 action against the Bank of Dandong prohibit covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, North Korean banking institutions and the Bank of Dandong.[14] Under these Section 311 actions, covered financial institutions must take reasonable steps to not process a transaction for the correspondent account of a foreign bank in the United States if such a transaction involves a North Korean financial institution.

Special Due Diligence of Correspondent Accounts

31 CFR § 1010.659 and 1010.660 also require covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving North Korean financial institutions and Bank of Dandong. At a minimum, that special due diligence must include:

- Notifying those foreign correspondent account holders, which the covered financial institution knows or has reason to believe provide services to a North Korean financial institution and Bank of Dandong, that they may not provide a North Korean financial institution or Bank of Dandong with access to the correspondent account maintained at the covered financial institution;[15] and

14. *See* 81 FR 35441 (June 2016), 31 CFR § 1010.659 and 31 CFR § 1010.660. *See* Footnote 5.

15. 31 CFR § 1010.659(b)(3)(i)(A) and 31 CFR § 1010.660(b)(3)(i)(A).

© gettechnical inc 2021

- Taking reasonable steps to identify any use of its foreign correspondent accounts by a North Korean financial institution or Bank of Dandong, to the extent that such use can be determined from transactional records maintained in the covered financial institution's normal course of business.[16]

Covered financial institutions shall take a risk-based approach when deciding what, if any, other due diligence measures it reasonably must adopt to guard against the use of its foreign correspondent accounts to process transactions involving North Korean financial institutions or Bank of Dandong.[17]

Covered financial institutions that know or have reason to believe that a foreign bank's correspondent account has been or is being used to process transactions involving a North Korean financial institution or Bank of Dandong must take all appropriate steps to further investigate and prevent such access, including the notification of its correspondent account holder (as mentioned above) and, where necessary, termination of the correspondent account.[18]

Suspicious Activity Reporting

Consistent with suspicious activity reporting requirements in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report (SAR).[19]

The presence or absence of a red flag in any given transaction is not by itself determinative of whether a transaction is suspicious. Due to some similarities with legitimate financial activities, financial institutions may want to consider evaluating indicators of potential DPRK-related illicit activity in combination with other red flags and factors before making determinations of suspiciousness. Financial institutions are encouraged to use previous FinCEN advisories and guidance related to the DPRK as a reference when evaluating potential suspicious activity.[20] Financial institutions may also want to consider the specifics of their own risk profiles and business models as those relate to the guidance and red flags outlined in this advisory.

16. 31 CFR § 1010.659(b)(3)(i)(B) and 31 CFR § 1010.660(b)(3)(i)(B).
17. 31 CFR § 1010.659(b)(3)(ii) and 31 CFR § 1010.660(b)(3)(ii).
18. 31 CFR § 1010.659(b)(3)(iii) and 31 CFR § 1010.660(b)(3)(iii).
19. 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
20. FinCEN Advisories pertaining to the DPRK: FIN-2013-A005 (July 2013), FIN-2009-A002 (June 2009), and FinCEN Advisory – Issue 40 (December 2005).

© gettechnical inc 2021

In evaluating whether certain transactions are suspicious and related to North Korean illicit finance, financial institutions are encouraged to share information with one another, as appropriate, either for the purposes of filing a joint SAR or under Section 314(b) of the USA PATRIOT Act.[21] Section 314(b) establishes a voluntary information sharing mechanism allowing financial institutions to share information with one another regarding possible terrorist activity or money laundering and provides financial institutions with the benefit of a safe harbor from liability that might not otherwise exist with respect to the sharing of such information.[22]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov. *Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).* The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

21. *See* 31 CFR § 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2)(i), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2) regarding joint SAR sharing. See Pub. L. No. 107-56, § 314(b) promulgated under 31 CFR § 1010.540 regarding Section 314(b) voluntary information sharing.

22. For further guidance related to the 314(b) Program, please see FinCEN's Section 314(b) Fact Sheet and FIN-2009-G002 "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act" (June 2009).

© gettechnical inc 2021

FinCEN FIN-2017-A007: Advisory to Financial Institutions Regarding Disaster-Related Fraud (10/31/2017)

UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

ADVISORY

FIN-2017-A007 October 31, 2017

Advisory to Financial Institutions Regarding Disaster-Related Fraud

Financial Institutions should be aware of potential fraudulent activity related to disaster relief efforts.

This Advisory should be shared with:

- *Chief Risk Officers*
- *Chief Compliance Officers*
- *Legal Departments*
- *AML/BSA Departments*
- *AML/BSA Analysts*
- *Fraud Departments*

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to warn financial institutions about the potential for fraudulent transactions in the wake of disasters, including recent hurricanes and wild fires. This advisory is not intended to deter legitimate donations and relief assistance efforts. Rather, the purpose is to help financial institutions identify and prevent fraudulent activity that may interfere with legitimate relief efforts.

The U.S. Department of Justice established the National Center for Disaster Fraud (NCDF) to investigate, prosecute, and deter fraud in the wake of Hurricane Katrina, when billions of dollars in federal disaster relief poured into the Gulf Coast region.[1] Its mission has expanded to include suspected fraud from any natural or manmade disaster, including Hurricanes Harvey, Irma, and Maria. More than 30 federal, state, and local agencies participate in the NCDF, which allows the NCDF to act as a centralized clearinghouse of information related to disaster relief fraud of all types. Financial institutions are encouraged to use the resources made available by the NCDF to help identify and mitigate their potential for all types of disaster fraud risks.

Potential Frauds

While there are many indicators of general fraud, financial institutions should pay particular attention to benefits fraud, charities fraud, and cyber-related fraud.

Benefits Fraud

Benefits fraud typically occurs when individuals apply for emergency assistance benefits to which they are not entitled. Financial institutions are at risk when fraudsters seek to deposit or obtain cash derived from the emergency assistance payments. FinCEN has noted an increase in the use of wire transfers to perpetrate these frauds. In those situations, requests for withdrawals are made and funds are wired to bank accounts, where the fraudster immediately withdraws the funds.

1. *See* https://www.justice.gov/usao-sdtx/pr/authorities-announce-formation-working-group-fight-hurricane-harvey-related-illegal

© gettechnical inc 2021

The NCDF has identified certain possible signs of fraudulent activity that may assist financial institutions in identifying and combating hurricane-related benefit fraud, including the following red flags:

- Deposits of multiple Federal Emergency Management Agency (FEMA), Red Cross, or other emergency assistance checks or electronic funds transfers into the same bank account, particularly when the amounts of the checks are the same or approximately the same (e.g., $2,000 or $2,358);
- Cashing of multiple emergency assistance checks by the same individual;
- Deposits of one or more emergency assistance checks, when the accountholder is a retail business and the payee/endorser is an individual other than the accountholder; and
- Opening of a new account with an emergency assistance check, where the name of the potential accountholder is different from that of the depositor of the check.

The presence or absence of a red flag in any given transaction is not by itself determinative of whether a transaction is suspicious. Financial institutions should take into account all relevant details of a customer or transaction and should not necessarily presume suspicious activity based on a single red flag.

Charities Fraud

Charities provide a vehicle for donations to assist hurricane victims. However, during times of disaster, criminals seek to exploit these vehicles for their own gain. Both legitimate and fraudulent contribution solicitations and schemes can originate from social media, e-mails, websites, door-to-door collections, flyers, mailings, telephone calls, and other similar methods. In the coming weeks and months, it is likely that millions of aid dollars will flow to areas affected by Hurricanes Harvey, Irma, and Maria.

To ensure those contributions end up where donors intend, and not in the hands of criminals, the NCDF has identified possible signs of fraudulent activity to assist financial institutions in identifying and combating hurricane-related charities fraud,[2] which may include the following red flags:

- Financial institutions may be able to identify potential fraudulent transactions where the payee organization's name is similar to, but not exactly the same as, those of reputable charities; or
- The use of money transfer services for charitable collections – generally, legitimate charities do not solicit donations via money transfer services.

2. *See* https://www.justice.gov/opa/pr/tips-avoiding-fraudulent-charitable-contribution-schemes

© gettechnical inc 2021

Cyber-Related Fraud

Cyber actors take advantage of public interest during natural disasters in order to conduct financial fraud and disseminate malware. The Center for Internet Security expects this trend to continue as new and recycled scams emerge involving financial fraud and malware related to Hurricanes Harvey, Irma, and Maria. As of September 2017, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed the registration of more than 743 domain names containing the word "Irma," and most include a combination of the words "help," "relief," "victims," "recover," "claims," or "lawsuits." They believe more domain registrations related to Hurricanes Harvey, Irma, and Maria are likely to follow.[3] Financial institutions may want to be aware of public reporting on hurricane-related or wild fire phishing campaigns, malicious websites, and associated malware. Institutions should be aware of the following red flags for potential cyber-related fraud:

- Crowdfunding platforms also can be exploited by criminal elements. While many crowdfunding efforts are legitimate and have platforms with the appropriate protections in place, some platforms have limited policies and procedures in place to protect customer funds and identification. In these circumstances, financial institutions should be aware of the risk this can present for potential identity theft vulnerabilities of account holders who are donors. Information security units in financial institutions may have access to information that may help in the detection and reporting of such activity.

- Some illicit crowdfunding sites are set up expressly to defraud donors. Cyber actors often create such sites using web designs or names that are virtually identical to legitimate charities and relief organizations to induce unwitting donors into making donations to criminal enterprises through these fraudulent sites. These fraudulent websites often end with a ".com" or a ".net", while most legitimate charities' websites end in ".org". For example, www.[charity].org (legitimate) versus www.[charity].net (potentially not legitimate). Payments to such websites may indicate fraudulent activity.

Financial institutions can report any internet-based fraud and crimes to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/.

Suspicious Activity Reporting

Consistent with suspicious activity reporting requirements in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report (SAR).[4]

3. *See* https://www.cisecurity.org/ms-isac/cyber-alert-cyber-threat-actors-expected-to-leverage-hurricane-irma/
4. 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

© gettechnical inc 2021

As noted above, the presence or absence of a red flag in any given transaction is not by itself determinative of whether a transaction is suspicious. Financial institutions should consider additional factors such as a customer's overall financial activity and whether it exhibits multiple red flags, as well as the specifics of their own risk profiles and business models as those relate to the information and red flags outlined in this advisory.

When evaluating potential suspicious activity, financial institutions should also be mindful that some red flags may be observed during general transactional monitoring, whereas others may be more readily identified during in-depth case reviews.

FinCEN requests, though does not require, that financial institutions reference this advisory and include the key term, "***Disaster-related Fraud***" in the SAR narrative and in SAR field 31(z) (Fraud-Other) to indicate a connection between the suspicious activity being reported and possible misuse of relief funds. Financial institutions should provide a detailed description of the known or suspected criminal violation or suspicious activity in the narrative sections of Suspicious Activity Reports.

If financial institutions encounter any of these situations, or other situations that they suspect may involve hurricane or other disaster-related benefit fraud or other potentially illicit transactions, they should complete and file a Suspicious Activity Report and, in these instances, also contact their local office of the Federal Bureau of Investigation or the United States Secret Service.[5]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov. ***Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day)***. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

5. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2)(i), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2) regarding joint SAR sharing. See Pub. L. No. 107-56, § 314(b) promulgated under 31 CFR § 1010.540 regarding Section 314(b) voluntary information sharing.

© gettechnical inc 2021

FinCEN FIN-2017-A003: Advisory to Financial Institutions and Real Estate Firms and Professionals (8/22/2017)

UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

ADVISORY

FIN-2017-A003 August 22, 2017

Advisory to Financial Institutions and Real Estate Firms and Professionals

Drug traffickers, corrupt officials, money launderers, and other criminals seek to exploit real estate transactions to hide their illicit profits, conceal their identities, and launder funds.

This Advisory should be shared with:

- *Real Estate Professionals*
- *Organization Executives*
- *Comptroller/Treasury/ Accounting Departments*
- *Compliance Departments*
- *Legal Departments*

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to provide financial institutions and the real estate industry with information on money laundering risks associated with certain real estate transactions. As highlighted by recent Geographic Targeting Orders (GTOs) issued by FinCEN, real estate transactions involving luxury property purchased through shell companies—particularly when conducted with cash and no financing—can be an attractive avenue for criminals to launder illegal proceeds while masking their identities.[1]

Each type of financial institution—defined by law to also include "persons involved in real estate closings and settlements"—has certain anti-money laundering obligations and can provide valuable reporting on potential money laundering and terrorist financing.[2] While real estate brokers, escrow agents, title insurers, and other real estate professionals are not required to, FinCEN encourages them to voluntarily report suspicious transactions involving real estate purchases and sales. As with other financial institutions under the Bank Secrecy Act (BSA), a safe harbor from liability exists with respect to the filing of suspicious activity reports, including voluntary ones, by persons involved in real estate closings and settlements.[3]

1. Although FinCEN to date has focused on residential real estate, money laundering can also involve commercial real estate transactions.
2. FinCEN—a bureau of the U.S. Department of the Treasury—administers and issues regulations pursuant to the Bank Secrecy Act (BSA). The BSA is the commonly used term for statutory enactments requiring U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering, terrorism finance, and other illegal activity. The BSA's definition of "financial institution" includes "persons involved in real estate closings and settlements." 31 U.S.C. § 5312(a)(2)(U). While that term has not yet been defined under FinCEN's regulations, it is not intended to include individual buyers and sellers.
3. *See* 31 U.S.C. § 5318(g)(3).

© gettechnical inc 2021

Money Laundering Risks in the Real Estate Sector

Real estate transactions and the real estate market have certain characteristics that make them vulnerable to abuse by illicit actors seeking to launder criminal proceeds. For example, many real estate transactions involve high-value assets, opaque entities, and processes that can limit transparency because of their complexity and diversity. In addition, the real estate market can be an attractive vehicle for laundering illicit gains because of the manner in which it appreciates in value, "cleans" large sums of money in a single transaction, and shields ill-gotten gains from market instability and exchange-rate fluctuations.[4] For these reasons and others, drug traffickers, corrupt officials, and other criminals can and have used real estate to conceal the existence and origins of their illicit funds.

Example: Corruption and Residential Real Estate

A high-profile case illustrating money laundering risks in the real estate sector involves 1Malaysia Development Berhad (1MDB), a Malaysian sovereign wealth fund. In 2016, the U.S. Department of Justice sought forfeiture of over $1 billion in assets—including luxury real estate—associated with funds stolen by corrupt foreign officials from 1MDB. This included a hotel, two homes, and a mansion in Beverly Hills, CA; a home in Los Angeles, CA; a condominium, two apartments, and a penthouse in New York, NY; and, a townhouse in London, England; all with a collected value estimated at approximately $315 million.

This money laundering risk in the real estate market was a principal driver of FinCEN's decision to issue GTOs, which, as described below, have provided greater insight into illicit finance risks in the high-end real estate market. FinCEN's analysis of BSA and GTO reported data, law enforcement information, and real estate deed records, as depicted by the case studies in this advisory, indicates that high-value residential real estate markets are vulnerable to penetration by foreign and domestic criminal organizations and corrupt actors, especially those misusing otherwise legitimate limited liability companies or other legal entities to shield their identities. In addition, when these transactions are conducted without any financing (*i.e.*, "all-cash"), they can potentially avoid traditional anti-money laundering (AML) measures adopted by lending financial institutions, presenting increased risk.

FinCEN encourages both financial institutions subject to mandatory suspicious reporting requirements, as well as real estate professionals filing voluntary suspicious activity reports, to keep the risks detailed below in mind when identifying and reporting suspicious transactions.

4. Money laundering is a crime orchestrated to conceal the source of illegal proceeds so that the money can be used without detection of its criminal source. Visit www.fincen.gov for further information.

© gettechnical inc 2021

Use of Shell Companies Decreases Transparency

Criminals launder money to obscure the illicit origin of their funds. To this end, money launderers can use a number of vehicles to reduce the transparency of their transactions. One such vehicle, highlighted in the below case study, is the use of shell companies. Shell companies are typically non-publicly traded corporations, limited liability companies (LLCs), or trusts that have no physical presence beyond a mailing address and generate little to no independent economic value.[5] Most shell companies are formed by individuals and businesses for legitimate purposes, such as to hold stock or assets of another business entity or to facilitate domestic and international currency trades, asset transfers, and corporate mergers. Shell companies can often be formed without disclosing the individuals that ultimately own or control them (*i.e.*, their beneficial owners) and can be used to conduct financial transactions without disclosing their true beneficial owners' involvement. Criminals abuse this anonymity to mask their identities, involvement in transactions, and origins of their wealth, hindering law enforcement efforts to identify individuals behind illicit activity.[6]

Example: Drug Trafficking, Luxury Real Estate, and Shell Companies

An example of abuse of the luxury real estate sector involves current Venezuelan Vice President Tareck El Aissami and his frontman Samark Lopez Bello. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated El Aissami under the Foreign Narcotics Kingpin Designation Act for playing a significant role in international narcotics trafficking. Lopez Bello was designated for providing material assistance, financial support, or goods or services in support of the international narcotics trafficking activities of, and acting for or on behalf of, El Aissami.[7] In addition, OFAC designated shell companies tied to Lopez Bello that were used to hold real estate.[8] Lopez Bello is tied to significant property and other assets, which were also blocked as a result of OFAC's action.

The misuse of shell companies to launder money is a systemic concern for law enforcement and regulatory agencies, but it is of particular concern in the "all-cash" segment of the real estate market, which currently has fewer AML protections.

5. For further information on shell companies, see FinCEN Guidance FIN-2006-G014 "Potential Money Laundering Risks Related to Shell Companies" (November 2006) and FinCEN's SAR Activity Review Trends, Tips, and Issues: Issue 1 (October 2000), Issue 2 (June 2001), and Issue 7 (August 2004).
6. In May 2018, many financial institutions will be required to implement customer due diligence obligations and collect beneficial ownership information on their legal entity customers at account opening. See, 81 Fed. Reg. 91 (May 2016).
7. *See* "Treasury Sanctions Prominent Venezuelan Drug Trafficker Tareck El Aissami and His Primary Frontman Samark Lopez Bello" (February 2017).
8. *Id.* Generally, under U.S. law, the assets and accounts of a designated individual, entity, or country must be frozen or blocked by U.S. individuals or entities.

© gettechnical inc 2021

Use of "All-Cash" Real Estate Purchases Further Decreases Transparency

Criminals can use all-cash purchases to make payments in full for properties and evade scrutiny—on themselves and the origin of their wealth—that is regularly performed by financial institutions in transactions involving mortgages.[9] All-cash transactions account for nearly one in four residential real estate purchases, totaling hundreds of billions of dollars nationwide, and are particularly exposed to abuse.[10] All-cash transactions account for an even larger stake in some U.S. markets. For instance, nearly 50 percent of residential real estate sales in Miami-Dade County were all-cash transactions in 2015 and 2016.[11] Many all-cash transactions are routine and legitimate, however, they also present significant opportunities for exploitation by illicit actors.

Example: Fraud, Money Laundering, and All-Cash Purchases

An example highlighting fraud and money laundering through all-cash transactions involves real estate agent Anthony Keslinke, who in 2016 was jailed, ordered to pay $1,427,916 in restitution to victims, and forfeited $3,808,831. Keslinke was the leader of both a large-scale bank fraud conspiracy and a separate money laundering conspiracy. Between 2011 and 2014, Keslinke used straw buyers and altered records and documents to purchase real estate with cash throughout Northern California, which he then resold at significant financial gain.[12]

FinCEN's Geographic Targeting Orders (GTOs)

In 2016 and 2017, FinCEN issued GTOs to better understand the vulnerabilities presented by the use of shell companies to engage in all-cash residential real estate transactions. A GTO is an order issued by FinCEN under the BSA that imposes additional recordkeeping or reporting requirements on financial institutions or other businesses in a specific geographic area.[13] In this case, FinCEN issued GTOs requiring certain U.S. title insurance companies to record and report information, including beneficial ownership, about legal entities used to make non-financed purchases of high-value residential real estate in seven major U.S. geographic areas.[14]

9. The BSA and FinCEN regulation generally require covered financial institutions—including those providing financing—to conduct diligence on their customers and their source of wealth.
10. The National Association of Realtors (NAR) consistently reports monthly figures on all-cash sales for existing homes to near 25 percent. *See* http://www.realtor.org/topics/existing-home-sales.
11. *See* the Miami Association of Realtors' 2016 Yearly Market Summaries for Single Family Homes and Townhouses and Condos.
12. *See* the Internal Revenue Service's (IRS) "Examples of Money Laundering Investigations – Fiscal Year 2016."
13. *See* 31 U.S.C. § 5326(a), 31 CFR § 1010.370, and Treasury Order 180-01.
14. *See* "GTOs Involving Certain Real Estate Transactions Frequently Asked Questions" (August 2016), "FinCEN Renews Real Estate "GTOs" to Identify High-End Cash Buyers in Six Major Metropolitan Areas" (February 2017), and "FinCEN Targets Shell Companies Purchasing Luxury Properties in Seven Major Metropolitan Areas" (August 2017).

© gettechnical inc 2021

As of May 2, 2017, over 30 percent of the real estate transactions reported under the GTOs involved a beneficial owner or purchaser representative that had been the subject of unrelated Suspicious Activity Reports (SARs) filed by U.S. financial institutions. In other words, the beneficial owners or purchaser representatives in a significant portion of transactions reported under the GTO had been previously connected to a wide array of suspicious activities, including:

- A beneficial owner suspected of being connected to over $140 million in suspicious financial activity since 2009 and who sought to disguise true ownership of related accounts.
- Two beneficial owners (husband and wife) involved in a $6 million purchase of two condominiums were named in nine SARs filed from 2013 – 2016 in connection with allegations of corruption and bribery associated with South American government contracts.
- A beneficial owner suspected of being connected to a network of individuals and shell companies that received over $6 million in wire transfers with no clear business purpose from entities in South America. Much of these funds were used for payments to various real estate related businesses.
- Eleven SARs filed from 2008 through 2015 named either the buyer (an LLC), beneficial owner, or purchaser's representative involved in a GTO-reported $4 million purchase of a residential unit. Law enforcement records indicate that both the purchaser's representative and his business associate were associated with a foreign criminal organization involved in narcotics smuggling, money laundering, health care fraud, and the illegal export of automobiles.

Review of U.S. Anti-Money Laundering Regulations in the Real Estate Sector

The real estate sector is one of many within the U.S. economy for which anti-money laundering (AML) safeguards have been established to protect the U.S. financial system.[15] More specifically, covered financial institutions—including depository institutions, loan or finance companies, and housing government-sponsored enterprises like Fannie Mae and Freddie Mac—generally have obligations to establish AML programs, report suspicious activity to FinCEN using Suspicious Activity Reports (SARs), and understand their customers and their source of wealth. In addition, beginning in May 2018, many financial institutions will be required to implement customer due diligence obligations and collect beneficial ownership information on their legal entity customers opening accounts.[16] FinCEN provides substantial guidance and information on how to implement these requirements effectively.[17]

15. 31 U.S.C. § 5318(h) requires financial institutions, including "persons involved in real estate closings and settlements," to establish an anti-money laundering program that includes, at a minimum: (A) the development of internal policies, procedures, and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs.
16. 81 Fed. Reg. 91 (May 2016).
17. For additional information, see https://www.fincen.gov/resources/financial-institutions/mortgage-co-broker.

© gettechnical inc 2021

While FinCEN currently has exempted them from these broader obligations, persons involved in real estate closings and settlements do participate in efforts to safeguard the U.S. real estate industry and financial system from money laundering and terrorism financing through their existing AML/CFT requirements.[18] They, like all U.S. persons engaged in trade and business, must file reports on transactions in currency and certain monetary instruments involving more than $10,000 (commonly referred to as "Form 8300").[19] They also may be required to annually report on foreign bank and financial accounts they own or control, report the transportation of currency across the U.S. border, and keep associated records, as well as respond to FinCEN-issued GTOs.[20] In addition, as other financial institutions under the BSA, persons involved in real estate closings and settlements—which may include real estate brokers, escrow agents, title insurers, and other real estate professionals—can voluntarily report suspicious activity and such disclosures would be protected from liability under the BSA's safe harbor.

The real estate industry recognizes the seriousness and importance of protecting the U.S. real estate market from abuse. For example, the National Association of Realtors has issued red flags and voluntary guidelines to assist real estate professionals minimize the risk of real estate becoming a vehicle for money laundering.[21]

Mandatory Reporting of Suspicious Activity

A covered financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from: illegal activity, attempts to disguise funds derived from illegal activity, is designed to evade regulations promulgated under the BSA, lacks a business or apparent lawful purpose, or involves the use of the financial institution to facilitate criminal activity.[22]

Voluntary Reporting of Suspicious Activity

SARs play an important role in assisting law enforcement to combat crime as they identify possible illicit activity and criminals. FinCEN encourages persons involved in real estate closings and settlements—which may include real estate brokers, escrow agents, title insurers, and other real estate professionals—to voluntarily file a SAR to report any suspicious transactions.[23] These persons are well-positioned to identify potentially illicit activity as they have access to a more complete view and understanding of the real estate transaction and of

18. *See* FinCEN's advance notice of proposed rulemaking "Anti-Money Laundering Program Requirements for 'Persons Involved in Real Estate Closings and Settlements'" (April 2003).
19. 31 CFR § 1010.330 (Form 8300). A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
20. 31 CFR §§ 1010.350 (FBAR), 1010.340 (CMIR), 1010.430 (recordkeeping), and 1010.370 (GTO).
21. *See* "Tips for Spotting Global Money Laundering Schemes" (January 2017) and "Anti-Money Laundering Guidelines for Real Estate Professionals" (November 2012).
22. 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
23. For instructions on how to file a SAR with FinCEN see https://www.fincen.gov/resources/filing-information.

© gettechnical inc 2021

those involved in the transaction. For example, real estate brokers may have greater insight as to the potential purpose for which a property is being purchased or the possible origin of a purchaser's funds. When reporting suspicious activity, persons involved in real estate closings and settlements should note that they can benefit from protection from civil liability.[24]

Real estate brokers, escrow agents, title insurers, and other real estate professionals can identify potential suspicious transactions by reviewing available facts and circumstances. Real estate professionals may determine a transaction is suspicious after evaluating whether the real estate transaction:

- Lacks economic sense or has no apparent lawful business purpose. Suspicious real estate transactions may include purchases/sales that generate little to no revenue or are conducted with no regard to high fees or monetary penalties;
- Is used to purchase real estate with no regard for the property's condition, location, assessed value, or sale price;
- Involves funding that far exceeds the purchaser's wealth, comes from an unknown origin, or is from or goes to unrelated individuals or companies; or
- Is deliberately conducted in an irregular manner. Illicit actors may attempt to purchase property under an unrelated individual's or company's name or ask for records (e.g., assessed value) to be altered.

Filing Suspicious Activity Reports (SARs)

To report suspicious transactions, financial institutions—including persons involved in real estate closings and settlements—should electronically submit a SAR through FinCEN's BSA E-Filing System. Additional information on how to complete and file a SAR is available at FinCEN's public website here.

When filing a mandatory or voluntary SAR involving a real estate transaction, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the real estate transaction and the circumstances and reasons why such transaction may be suspicious in the narrative section of the SAR.

FinCEN also requests that financial institutions reference this advisory and include the key term

"ADVISORY REAL ESTATE"

in the SAR narrative and in SAR field 33(z) (Money Laundering-Other) to indicate a connection between the suspicious activity being reported and real estate property.

24. *See* 31 U.S.C. § 5318(g)(3)(A). Persons filing SARs should also note that FinCEN protects the confidentiality of such filings.

© gettechnical inc 2021

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov, (800) 767-2825 (Option 9), or (703) 905-3591 (Option 9). ***Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

© gettechnical inc 2021

FINCEN ADVISORY: FIN-2016-A005 CYBER CRIMES (OCTOBER 25, 2016)

FIN-2016-A005
Issued Date: October 25, 2016
Subject: Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime

Cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats.

The proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system. The Financial Crimes Enforcement Network (FinCEN) issues this advisory to assist financial institutions in understanding their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

I. Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);

II. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;

III. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity; and

IV. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

For the purpose of this advisory:[1]

Cyber-Event: An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.
Cyber-Enabled Crime: Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.

For the purpose of this advisory (continued):

Cyber-Related Information: Information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs). Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

Background

© gettechnical inc 2021

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions can play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs.

Value of BSA Reporting in Combating Cybercriminals and Cyber-Enabled Crime

FinCEN and law enforcement regularly use information financial institutions report under the BSA to initiate investigations, identify criminals, and disrupt and dismantle criminal networks. The cyber-related information that financial institutions include in this reporting is a valuable source of investigatory leads. Law enforcement has been able to use cyber-related information reported—such as IP addresses with timestamps, cyber-event data, and virtual-wallet information—to track criminals, identify victims, and trace illicit funds.

For example, BSA reporting by more than 20 financial institutions—on transactions related to cyber-enabled crimes—played an important role in the investigation of an internet-based company, its co-founders, and other collaborators. This company acted as an unregistered online money-transmitting business and offered digital currency services specifically designed to provide anonymity to facilitate international crime and money laundering. Criminals used this company to conduct over $6 billion in illicit transactions involving proceeds from cyber-attacks, credit card fraud, child pornography, Ponzi schemes, identity theft, and trafficking in narcotics and other contraband.

Regulatory Expectations

This advisory does not change existing BSA requirements or other regulatory obligations for financial institutions.[2] Financial institutions should continue to follow federal and state requirements and guidance on cyber-related reporting and compliance obligations.[3]

Financial institutions should also note that filing a SAR does not relieve financial institutions from any other applicable requirements to timely notify appropriate regulatory agencies of events concerning critical systems and information or of disruptions in their ability to operate. In addition, the recently enacted Cybersecurity Act of 2015,[4] also known as the Cybersecurity Information Sharing Act (CISA), does not change any SAR-reporting requirements under the BSA,[5] SAR confidentiality rules,[6] or the safe harbor protections under section 314 of the USA PATRIOT Act.[7]

Guidance to U.S. Financial Institutions

The following guidance explains how BSA regulations and requirements apply to cyber-events, cyber-enabled crime, and cyber-related information.

I. SAR Reporting of Cyber-Events

Cyber-events targeting financial institutions often constitute criminal activity and can serve as means to commit a wide range of further criminal activity.[8] For instance, criminals may seek to obtain unauthorized electronic access to electronic systems, services, resources, or information to conduct unauthorized transactions. Cyber-events can target or

affect funds directly—such as in cases of fraud, identity/credential theft, and misappropriation of funds. Similarly, cyber-events can generate illicit proceeds—such as in cases of ransomware attacks and the sale of stolen proprietary information and credit card numbers.

Mandatory SAR reporting of cyber-events

A financial institution is required to report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets.[9] If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.

In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.[10]

Financial institutions should also be familiar with any other cyber-related SAR-filing obligations required by their functional regulator. For instance, the Office of the Comptroller of the Currency (OCC) requires national banks to file SARs to report unauthorized electronic intrusions.[11] The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) issued guidance concerning the filing of SARs to report certain computer-related crimes.[12]

The following examples illustrate situations in which SAR reporting of cyber-events is mandatory. These examples do not, however, describe all instances when cyber-events require the filing of a SAR.

Example 1: Through a malware intrusion (a type of cyber-event), cybercriminals gain access to a bank's systems and information. Following its detection, the bank determines the cyber-event put $500,000 of customer funds at risk, based on the systems and/or information targeted by the cyber-event. Accordingly, the bank reasonably suspects the intrusion was in part intended to enable the perpetrators to conduct unauthorized transactions using customers' funds.

The bank must file a SAR because it has reason to suspect the cybercriminals, through the malware-intrusion, intended to conduct or could have conducted unauthorized transactions aggregating or involving at least $5,000 in funds or assets. As explained in the next section, the bank should include all available information in the SAR relevant to the suspicious activity, including cyber-related information such as a description and signatures of the cyber-event, attack vectors, command-and-control nodes, etc.

Example 2: Through a cyber-event, cybercriminals gain access to a financial institution's systems/networks. The cyber-event exposes sensitive customer information such as

© gettechnical inc 2021

account numbers, credit card numbers, balances, limits, scores, histories, online-banking credentials, passwords/PINs, challenge questions and answers, or other similar information useful or necessary to conduct, affect, or facilitate transactions.

By evaluating the cyber-event and the type of information sought by its perpetrators, the financial institution reasonably suspects the cyber-event may have targeted information for the purpose of conducting, facilitating, or affecting transactions aggregating to at least $5,000. For instance, the financial institution could reasonably suspect the cybercriminals intended to steal and sell the exposed sensitive customer information to other criminals for financial exploitation to include unauthorized transactions at the institution. As further described below, the targeted financial institution should file a SAR to report all relevant information, including cyber-related information and information pertaining to any related unauthorized transactions.

Examples 1 and 2 describe instances where a financial institution should file a SAR in response to a cyber-event. Although no actual transactions may have occurred in these examples, the circumstances of the cyber-events and the systems and information targeted could reasonably lead the financial institutions to suspect the events were intended to be part of an attempt to conduct, facilitate, or affect an unauthorized transaction or series of unauthorized transactions aggregating or involving at least $5,000 in funds or assets.

Example 3: A Money Services Business (MSB) knows or suspects a Distributed Denial of Service (DDoS) attack prevented or distracted its cybersecurity or other appropriate personnel from immediately detecting or stopping an unauthorized $2,000 wire transfer.

In this case, the financial institution should file a single SAR to report both the unauthorized wire transfer and the related DDoS attack. The financial institution should report the transaction because it was unauthorized and meets the filing threshold; and it should report the DDoS attack because the DDoS attack was perpetrated to conceal the unauthorized wire transfer.

Voluntary reporting of cyber-events

FinCEN encourages, but does not require, financial institutions to report egregious, significant, or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR.

To illustrate, consider a DDoS attack that disrupts a financial institution's website and disables the institution's online banking services for a significant period of time. After mitigating and investigating the DDoS attack, the affected financial institution determines the attack was not intended to and could not have affected any transactions. Although a financial institution is not required to report such DDoS attack, FinCEN encourages the financial institution to consider filing a SAR because the attack caused online banking disruptions that were particularly damaging to the institution. SAR reporting of cyber-events, even those that may not meet mandatory SAR-filing requirements, is highly valuable in law enforcement investigations.

II. Including Cyber-Related Information in SAR Reporting

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information. Because everyday financial transactions increasingly rely on electronic systems and resources, illicit financial

© gettechnical inc 2021

activity often has a digital footprint, which may correspond to illicit actors and their associates, their activity, and related suspicious transactions.

Thus, financial institutions should include available cyber-related information when reporting *any* suspicious activity, including those related to cyber events as well as those related to other activity, such as fraudulent wire transfers. Cyber-related information includes, but is not limited to, IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information. FinCEN also encourages the filing of all such cyber-related information when a financial institution files a voluntary SAR. For additional information on reporting cyber-related information in SARs, please refer to these Frequently Asked Questions (FAQs) available on FinCEN's website.

Reporting cyber-related information involving cyber-events

When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR—in addition to any other related suspicious activity. As needed, financial institutions may also attach a comma separated value (CSV) file to SARs to report data, such as cyber-event data and transaction details, in tabular form.[13] For example, to the extent available, SARs involving cyber-events should include:

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

Financial institutions subject to large numbers of cyber-events may report them through a single cumulative SAR filing when such events are similar in nature. For instance, a financial institution may file one SAR to report several malware intrusions if these events share common characteristics and indicators such as the methodology used, the vulnerability exploited, and IP addresses involved.[14]

FinCEN also encourages financial institutions to incorporate cyber-related information into their BSA/AML monitoring efforts and report relevant cyber-related information in SARs. In the event a financial institution's filing software is not yet capable of including certain relevant information such as cyber-related information, as clarified by FinCEN in May 2013, the institution should manually complete discrete SAR filings until it updates its software to allow the inclusion of such information.[15] Financial institutions can submit discrete SARs through FinCEN's BSA E-Filing System .

This advisory is not intended to, and does not, create any new obligation or expectation requiring financial institutions to collect cyber-related information as a matter of course.

III. Collaboration between BSA/AML and Cybersecurity Units

As the examples above illustrate, collaboration and ongoing communication among BSA/AML, cybersecurity, and other units will help financial institutions conduct a more

comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime. Accordingly, financial institutions are encouraged to internally share relevant information from across the organization, including, as appropriate, with BSA/AML staff, cybersecurity personnel, fraud prevention teams, and other potentially affected units.

Information provided by cybersecurity units could reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units. For instance, BSA/AML units can use cyber-related information, such as patterns and timing of cyber-events and transaction instructions coded into malware among other things, to (1) to help identify suspicious activity and criminal actors and (2) develop a more comprehensive understanding of their BSA/AML risk exposure. Likewise, cybersecurity personnel can use information provided by BSA/AML units to help the institution guard against cyber-events and cyber-enabled crime. In addition, this type of internal cooperation provides for more comprehensive and complete SAR reporting and is consistent with the principles involved in establishing a strong culture of compliance.[16]

IV. Sharing Cyber-Related Information between Financial Institutions

Financial institutions can work together to identify threats, vulnerabilities, and criminals. By sharing information with one another, financial institutions may gain a more comprehensive and accurate picture of possible threats, allowing for more precise decision making in risk mitigation strategies. FinCEN continues to encourage financial institutions to use all lawful means to guard against money laundering and terrorist activities presented through cyber-events and cyber-enabled crime.

To encourage information sharing, Section 314(b) of the USA PATRIOT Act extends a safe harbor from liability to financial institutions—after notifying FinCEN and satisfying certain other requirements—that voluntarily share information with one another for the purpose of identifying and, where appropriate, reporting potential money laundering or terrorist activities.[17] Under Section 314(b), financial institutions may share information, including cyber-related information, regarding individuals, entities, organizations, and countries for the purposes of identifying and reporting money laundering and terrorist activities. Thus, financial institutions may receive 314(b) safe harbor protections when sharing cyber-related information for the above mentioned purposes.[18]

Cyber-related information, such as information about specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses, for example, can help identify the individuals, entities, organizations, or countries involved or responsible for the cyber-event or cyber-enabled crime linked to money laundering or terrorist activities.

For Immediate Assistance, Contact Regulatory and Law Enforcement Agencies

Financial institutions needing immediate assistance in the event of a cyber-event or a cyber-enabled crime should contact appropriate regulatory and law enforcement agencies. Regulatory and law enforcement agencies can help affected financial institutions normalize systems and operations and, in some cases, reduce monetary losses. The U.S. Department of Homeland Security (DHS) published a fact sheet on obtaining threat and asset response assistance following a cyber incident.[19] In addition, the U.S. Department of

© gettechnical inc 2021

Justice published a guide outlining appropriate government agencies to contact in the event of computer hacking, fraud, and other internet-related crime.[20]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov , (800) 767-2825 (Option 9), or (703) 905-3591 (Option 9). ***Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

###

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

---

[1] Unless otherwise defined by FinCEN, FinCEN uses the Glossary of Key Information Security Terms and other publications issued by the National Institute of Standards and Technology (NIST) for definitions of cyber-related terms. NIST is a non-regulatory federal agency within the U.S. Department of Commerce. Financial Institutions are encouraged to refer to the NIST Glossary for definitions.

[2] For previous guidance regarding cyber-related suspicious activity reporting, financial institutions may generally refer to: Suspicious Activity Report Instructions issued on June 2000, July 2003, and March 2011 (see in particular, instructions for when to make a report for unauthorized electronic intrusions a.k.a. computer intrusions); SAR Activity Review Trends, Tips, and Issues: Issue 3 (October 2001); FinCEN Advisory FIN-2011-A006 "Account Takeover Activity" (December 2011); and Frequently Asked Questions Regarding the FinCEN SAR (May 2013).

[3] Financial institutions supervised by the federal banking agencies may also refer to additional guidance such as the Federal Financial Institutions Examination Council (FFIEC) Joint Statement on Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources (April 2014); FFIEC Joint Statements on Destructive Malware and Compromised Credentials (March 2015); FFIEC Joint Statement on Cyber Attacks Involving Extortion (November 2015); and the FFIEC IT Examination Handbook .

[4] *See*, Pub. L. No. 114-113 and Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016). CISA authorizes, among other things, non-federal entities to share voluntarily specifically defined cyber-threat indicators and defensive measures for cybersecurity purposes.

[5] *See*, 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20; as well as, Guidance to Assist Non-Federal Entities to

Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016).

[6]*See*, 31 U.S.C. § 5318(g)(2).

[7]*See*, 31 C.F.R. § 1010.540.

[8]*See generally*, 18 U.S.C § 1030.

[9]*See*, 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000. 31 C.F.R. § 1022.320(a)(2).

[10] Guidance on the reporting of Unauthorized Electronic Intrusions (UEIs) remains unchanged; see supra note 2. Financial institutions should report cyber-events as UEIs when such cyber-events meet the definition of a UEI. A UEI is defined as gaining access to a computer system of a financial institution to: a) remove, steal, procure or otherwise affect funds of the financial institution or the institution's customers; b) remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or c) damage, disable, disrupt, impair or otherwise affect critical systems of the financial institution.

[11]*See*, OCC Bulletin OCC 2000-14 "Infrastructure Threats—Intrusion Risks " (May 2000).

[12]*See*, FRB Supervisory Letter SR 97-28 "Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions " (November 1997); FDIC Financial Institution Letter FIL-124-97 "Guidance for Financial Institutions on Reporting Computer-Related Crimes " (December 1997); and NCUA Regulatory Alert 97-RA-12 "Guidance for Reporting Computer-Related Crimes " (December 1997).

[13] A CSV file is a part of, but not a substitute for, the SAR narrative. In addition, like other information prepared in connection with a SAR filing but not attached to a SAR, an unattached CSV file is considered supporting documentation and should be accorded confidentiality to the extent it indicates the existence of a SAR.

[14] See FAQs regarding the Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs (October 2016).

[15] See Frequently Asked Questions Regarding the FinCEN SAR (May 2013).

[16]*See,* FinCEN Advisory FIN-2014-A007 "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (October 2014).

[17] For further information regarding Section 314(b), including requirements for sharing information, please refer to the Section 314(b) Fact Sheet available on FinCEN's website.

[18] For information on sharing cyber-related information outside BSA safe harbor protections, please see the Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 .

[19] The DHS fact sheet was issued pursuant to Presidential Policy Directive 41, which sets forth principles governing the Federal Government's response to any cyber incident,

© gettechnical inc 2021

whether involving government or private sector entities. The DHS fact sheet also lists key points of federal contact and is available at https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf .

[20] Available at the Department of Justice website at https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime .

© gettechnical inc 2021

FINCEN FIN-2016-A003: ADVISORY TO FINANCIAL INSTITUTIONS ON E-MAIL COMPROMISE FRAUD SCHEMES (9/6/2016)

Criminals are actively using e-mail schemes to defraud financial institutions and their customers—billions of dollars in possible losses.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help financial institutions guard against a growing number of e-mail fraud schemes in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers. This advisory also provides red flags—developed in consultation with the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS)—that financial institutions may use to identify and prevent such e-mail fraud schemes.

E-mail Compromise Fraud: Schemes in which criminals compromise the e-mail accounts of victims to send fraudulent wire transfer instructions to financial institutions in order to misappropriate funds. The main types of e-mail compromise fraud include:

- ***Business E-mail Compromise (BEC):*** Targets a financial institution's commercial customers.
- ***E-mail Account Compromise (EAC):*** Targets a victim's personal accounts.

BEC and EAC schemes are among the growing trend of cyber-enabled crime adversely affecting financial institutions. Since 2013, there have been approximately 22,000 reported cases of BEC and EAC fraud involving $3.1 billion.[1] In some cases, financial institutions have absorbed losses through reimbursing customers victimized by e-mail compromise fraud. Financial institutions can play an important role in identifying, preventing, and reporting fraud schemes by promoting greater communication and collaboration among their internal anti-money laundering (AML), business, fraud prevention, and cybersecurity units.

This advisory should be shared with:

- *Cybersecurity departments*
- *Risk departments*
- *Fraud prevention units*
- *BSA/AML management*
- *AML intelligence units*
- *AML analysts/investigators*

How BEC and EAC Schemes Work

Unlike account takeover activity, e-mail-compromise schemes involve impersonating victims to submit seemingly legitimate transaction instructions for a financial institution to

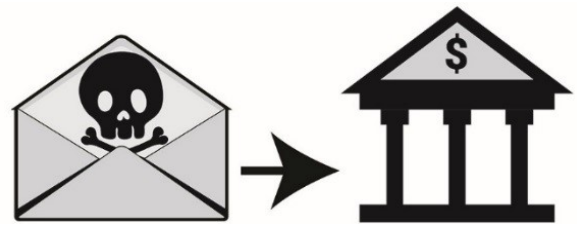
© gettechnical inc 2021

execute. In account takeover activity, criminals access victims' accounts and are able to directly execute transactions without submitting transaction instructions.[2]

While BEC and EAC schemes have unique aspects, as noted below, both focus on using compromised e-mail accounts to mislead financial institutions and their customers into conducting unauthorized wire transfers. Both BEC and EAC schemes can be broken down into three stages:

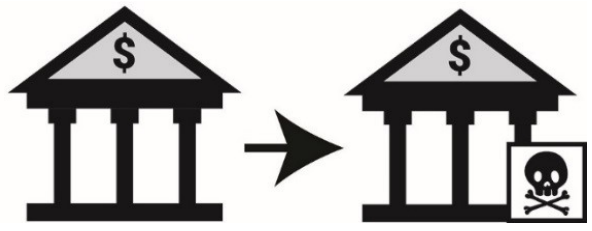
Stage 1 – Compromising Victim Information and E-mail Accounts:

Criminals first unlawfully access a victim's e-mail account through social engineering[3] or computer intrusion techniques. Criminals subsequently exploit the victim's e-mail account to obtain information on the victim's financial institutions, account details, contacts, and related information.



Stage 2 – Transmitting Fraudulent Transaction Instructions:

Criminals then use the victim's stolen information to e-mail fraudulent wire transfer instructions to the financial institution in a manner appearing to be from the victim. To this end, criminals will use either the victim's actual e-mail account they now control or create a fake e-mail account resembling the victim's e-mail.



Stage 3 – Executing Unauthorized Transactions:

Criminals trick the victim's employee or financial institution into conducting wire transfers that appear legitimate but are, in fact, unauthorized. The fraudulent transaction instructions

© gettechnical inc 2021

direct the wire transfers to the criminals' domestic or foreign bank accounts. Banks in Asia—particularly in China and Hong Kong—are common destinations for these fraudulent transactions.

Business E-Mail Compromise (BEC) Schemes

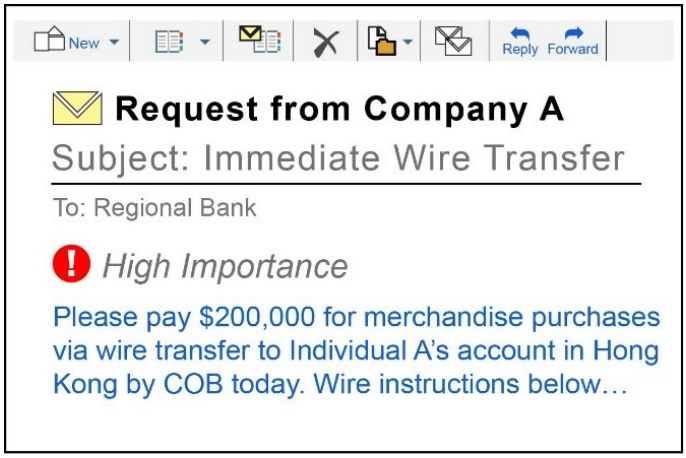
BEC schemes target financial institutions' commercial customers. Criminals seek to access unlawfully the e-mail accounts of a company's executives or employees to:

a. Directly submit fraudulent transaction instructions to the company's financial institution by impersonating company employees through e-mails and documentation related to the requested transfer; or
b. Mislead a company employee into submitting fraudulent transaction instructions to the company's financial institution by impersonating a supplier or a company executive to authorize or order payment through seemingly legitimate internal e-mails.

To illustrate, BEC schemes often take the following forms:

SCENARIO 1 – CRIMINAL IMPERSONATES A FINANCIAL INSTITUTION'S COMMERCIAL CUSTOMER:

A criminal hacks into and uses the e-mail account of a Company A employee to send fraudulent wire transfer instructions to Company A's financial institution. Based on this request, Company A's financial institution issues a wire transfer and sends funds to an account the criminal controls. *In this scenario, the criminal impersonating the financial institution's customer prompted the financial institution to execute an unauthorized wire transfer.*

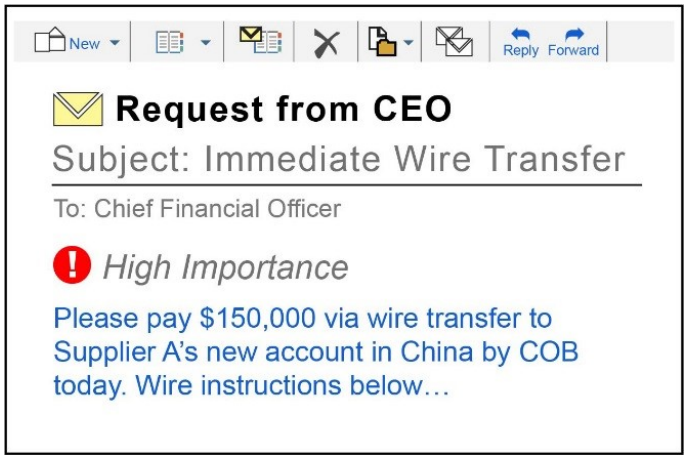


SCENARIO 2 – CRIMINAL IMPERSONATES AN EXECUTIVE:

A criminal hacks into and uses the e-mail account of a Company B executive to send wire transfer instructions to a Company B employee who is responsible for processing and issuing payments. The employee, believing the executive's e-mailed instructions are

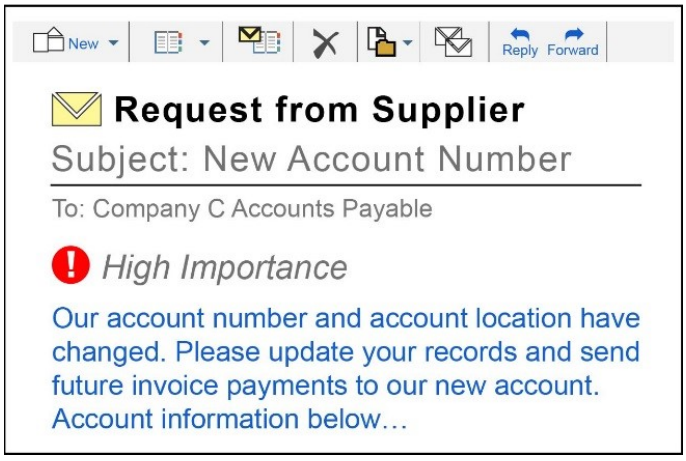
© gettechnical inc 2021

legitimate, orders Company B's financial institution to execute the wire transfer. *In this scenario, the criminal impersonating a company executive misled a company employee into unintentionally authorizing a fraudulent wire transfer to a criminal-controlled account.*



SCENARIO 3 – CRIMINAL IMPERSONATES A SUPPLIER:

A criminal impersonates one of Company C's suppliers to e-mail and inform Company C that future invoice payments should be sent to a new account number and location. Based on this fraudulent e-mailed information, Company C updates its supplier's payment information on record and submits the new wire transfer instructions to its financial institution that direct payments to an account controlled by the criminal. *In this scenario, the criminal impersonating a supplier provided fraudulent payment information to mislead a company employee into unintentionally directing wire transfers to a criminal-controlled account.*



E-Mail Account Compromise (EAC) Schemes

Unlike BEC, EAC schemes target individuals instead of businesses. Individuals who conduct large transactions through financial institutions, lending entities, real estate companies, and law firms are the most likely targets of this type of scheme. EAC schemes often take the following forms:

Scenario 1 – Lending/Brokerage Services: A criminal hacks into and uses the e-mail account of a financial services professional (such as a broker or accountant) to e-mail fraudulent instructions, allegedly on behalf of a client, to the client's bank or brokerage, to wire-transfer client's funds to an account controlled by the criminal.

Scenario 2 – Real Estate Services: A criminal compromises the e-mail account of a realtor or of an individual purchasing or selling real estate, for the purposes of altering payment instructions and diverting funds of a real estate transaction (such as sale proceeds, loan disbursements, or fees). Alternately, a criminal hacks into and uses a realtor's e-mail address to contact an escrow company, instructing it to redirect commission proceeds to an account controlled by the criminal.

Scenario 3 – Legal Services: A criminal compromises an attorney's e-mail account to access client information and related transactions. The criminal then e-mails fraudulent transaction payment instructions to the attorney's financial institution. Alternatively, the criminal may compromise a client's e-mail account to request wire transfers from trust and escrow accounts the client's attorney manages.

BEC and EAC Fraud Red Flags

Success in detecting and stopping BEC and EAC schemes requires careful review and verification of customers' transaction instructions and consideration of the circumstances surrounding such instructions.

In applying the red flags below, financial institutions are advised that *no single transactional red flag necessarily indicates suspicious activity.* Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity and whether the customer exhibits multiple red flags, before determining that a transaction is suspicious. Financial institutions should also perform additional inquiries and investigations where appropriate.

BEC and EAC schemes are similar and, therefore, may exhibit similar suspicious behavior, which can be identified by one or more of the following red flags:

- A customer's seemingly legitimate e-mailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.
- Transaction instructions originate from an e-mail account closely resembling a known customer's e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters. For example:

  Legitimate e-mail address

-

  john-doe@abc.com

© gettechnical inc 2021

Fraudulent e-mail addresses

- john_doe@abc.com
- john-doe@bcd.com

- E-mailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
- E-mailed transaction instructions direct wire transfers to a foreign bank account that has been documented in customer complaints as the destination of fraudulent transactions.
- E-mailed transaction instructions direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- E-mailed transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret," or "Confidential."
- E-mailed transaction instructions are delivered in a way that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- E-mailed transaction instructions originate from a customer's employee who is a newly authorized person on the account or is an authorized person who has not previously sent wire transfer instructions.
- A customer's employee or representative e-mails a financial institution transaction instructions on behalf of the customer that are based exclusively on e-mail communications originating from executives, attorneys, or their designees. However, the customer's employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.
- A customer e-mails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- A wire transfer is received for credit into an account, however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor, while thinking the new account belongs to the known supplier/vendor, as described in the above BEC Scenario 3. This red flag may be seen by financial institutions *receiving* wire transfers sent by another financial institution as the result of e-mail-compromise fraud.

Guidance to U.S. Financial Institutions

A multi-faceted transaction verification process can help financial institutions guard against BEC and EAC fraud. For instance, financial institutions may verify the authenticity of suspicious e-mailed transaction payment instructions by using multiple means of communication or by contacting others authorized to conduct the transactions. The success

© gettechnical inc 2021

of BEC and EAC schemes depends on criminals prompting financial institutions to execute seemingly legitimate but unauthorized transactions. Such transactions are often irrevocable, which renders financial institutions and their customers unable to cancel payment or recall the funds. Identifying fraudulent transaction payment instructions before payments are issued is therefore essential to preventing and reducing unauthorized transactions.

FinCEN has partnered with the FBI and the USSS to help financial institutions recover funds stolen as the result of BEC schemes. Through this partnership, FinCEN has successfully assisted in the recovery of hundreds of millions of dollars in the past year. While the recovery of BEC stolen funds is not assured, FinCEN has had greater success in recovering fundswhen victims or financial institutions report BEC-unauthorized wire transfers to law enforcement within 24 hours.

To request immediate assistance in recovering BEC-stolen funds, financial institutions should file a complaint with FBI's IC3 at www.ic3.gov , or contact the nearest USSS field office through www.secretservice.gov/field_offices.shtml . Contacting law enforcement for fund recovery assistance does not relieve a financial institution from its Suspicious Activity Report (SAR) filing obligations.

As further described below, financial institutions should be prepared to provide transactional details and cyber-related information surrounding the BEC scheme when requesting assistance in recovering funds.

SUSPICIOUS ACTIVITY REPORTING

A financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or *attempted* by, at, or through the financial institution involves funds derived from: illegal activity; attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the Bank Secrecy Act (BSA); lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[4] With respect to e-mail-compromise fraud, a financial institution may have a SAR filing obligation regardless of whether the scheme or involved transactions were successful, and regardless of whether the financial institution or its customers incurred an actual loss.[5]

When filing a SAR, financial institutions should provide all pertinent available information, including cyber-related information in the SAR form and narrative. Specifically, providing the following information is highly valuable to law enforcement and FinCEN in investigating BEC and EAC fraud:

Wire transfer details:

Scheme details:

- Dates and amounts of suspicious transactions;
- Sender's identifying information, account number, and financial institution;

© gettechnical inc 2021

- Beneficiary's identifying information, account number, and financial institution; and
- Correspondent and intermediary financial institutions' information, if applicable.
- Relevant e-mail addresses and associated Internet Protocol (IP) addresses with their respective timestamps and
- Description and timing of suspicious e-mail communications

Because some red flags associated with BEC and EAC fraud may actually reflect legitimate financial activities, financial institutions should evaluate indicators of potential BEC or EAC activity in combination with other red flags and the expected transaction activity before making determinations of suspiciousness. Due to the nature of BEC and EAC schemes, FinCEN encourages communication among financial institutions under the auspices of Section 314(b) of the USA PATRIOT Act in determining transactions' potential suspiciousness related to terrorist financing or money laundering activities, and in filing SARs, as appropriate.

FinCEN requests that financial institutions **reference this advisory and include the key terms:**

"BEC FRAUD" when **businesses** are the scheme victims

"EAC FRAUD" when **individuals** are the scheme victims

in the SAR narrative and in SAR field 31(z) (Fraud-Other) to to indicate a connection between the suspicious activity being reported and possible BEC or EAC fraud. Financial institutions should include one or both key terms to the extent they are able to distinguish between BEC and EAC fraud.

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov , (800) 767-2825 (Option 9), or (703) 905-3591 (Option 9). **Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day)**. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

---

[1] See the FBI Internet Crime Complaint Center (IC3) Public Service Announcement "Business Email Compromise: The 3.1 Billion Dollar Scam " (June 14, 2016) and 2015 Internet Crime Report .

[2] See FinCEN Advisory FIN-2011-A016 "Account Takeover Activity" (December 2011).

© gettechnical inc 2021

[3] Social engineering refers to human interaction tactics used to deceive an individual into revealing information.

[4] 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

[5] Id.

© gettechnical inc 2021

FINCEN ADVISORY: FIN-2014-A008 GUIDANCE ON RECOGNIZING ACTIVITY THAT MAY BE ASSOCIATED WITH HUMAN SMUGGLING AND HUMAN TRAFFICKING – FINANCIAL RED FLAGS (9/11/14)

FIN-2014-A008
ISSUED DATE: SEPTEMBER 11, 2014
SUBJECT: GUIDANCE ON RECOGNIZING ACTIVITY THAT MAY BE ASSOCIATED WITH HUMAN SMUGGLING AND HUMAN TRAFFICKING — FINANCIAL RED FLAGS

To support law enforcement efforts to fight human smuggling and human trafficking, the Financial Crimes Enforcement Network (FinCEN) seeks to advise financial institutions on how to detect and report suspicious financial activity that may be related to human smuggling and/or human trafficking. Financial institutions, large and small, can play a critical role in identifying and reporting transactions related to these unlawful activities based on their observations when interacting with customers and their monitoring processes.

FinCEN, in collaboration with law enforcement agencies, non-governmental organizations and members of the financial industry, has identified financial indicators, or "red flags," that may indicate financial activity related to human smuggling or human trafficking. In addition to identifying red flags, this advisory provides common terms that financial institutions may use when reporting activity related to these crimes. The use of common terms will assist law enforcement in better identifying possible cases of human smuggling or human trafficking reported through Suspicious Activity Reports (SARs).

Human Smuggling

Acts or attempts to bring unauthorized aliens to or into the United States, transport them within the U.S., harbor unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status.[1]

Human Trafficking

The act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force, fraud or coercion.[2]

Difference between Human Smuggling and Human Trafficking

Human Smuggling

(i) Involves persons choosing to immigrate illegally.
(ii) Is limited to illegal migration or the harboring of undocumented aliens.
(iii) Involves foreign nationals.
(iv) The crime involves an illegal border crossing or the harboring of someone that illegally crossed the border.

Human Trafficking

© gettechnical inc 2021

(i) Involves the use of force or coercion and the exploitation of victims.
(ii) Includes, but is not limited to, involuntary servitude, forced labor, debt bondage, peonage and sexual exploitation.
(iii) Anyone can be a victim regardless of origin, sex, age or legal status.
(iv) There is no need for a person to cross a border to be trafficked; individuals can be trafficked within the borders of a country.

Understanding How Human Smuggling and Human Trafficking Work

There are a number of identifiable stages involved in human smuggling and in human trafficking during which traffickers may need to interact with the financial system. This advisory includes below a brief description of these stages to provide financial institutions with the necessary context to appropriately identify potential human smuggling and/or human trafficking-related transactions. Financial indicators, including those described in Appendices A and B, may reflect transactions associated with actions that facilitate one or more of the stages of human smuggling and/or human trafficking.

How Human Smuggling Works

Stages of Human Smuggling generally include:

Solicitation: A potential migrant may seek the services of a local facilitator/smuggler. Local facilitators/smugglers are often part of a larger smuggling network that works to bring migrants across a country border. In the United States, illegal migrants often originate from Mexico and Central America, but they may originate from anywhere in the world.

Transportation: Migrants may be smuggled through a number of different routes and transportation modes to avoid detection. The person may be transported by air, sea and/or land over an international border.

Payment: Payment to smugglers or to smuggling networks are generally conducted in one of three ways.

1. *Pay In Advance*: The migrant or the migrant's relatives provide full payment to the smuggler before traveling. This method of payment is often used by relatives of unaccompanied minors for their migration.

2. *Partial Payment*: A portion of the smuggling fees is paid prior to departure, with the remaining due upon arrival; final payment is often made by relatives of the migrant in the United States.

3. *On Arrival*: After the migrant is successfully smuggled, the migrant's relatives pay the full fee to the smuggler. This method of payment is often used by relatives of unaccompanied minors for their migration.

How Human Smuggling Works

Stages of Human Smuggling generally include:

Recruitment or Abduction: Traffickers obtain their victims through deception or force. For instance, traffickers may recruit victims through the use of kidnapping, false marriages, or advertisements offering employment or study abroad. Individuals from countries and geographic areas that have been affected by economic hardship, armed conflicts or natural disasters are particularly vulnerable to these tactics.

Transportation: After being collected, victims are transported to locations where they are exploited or sold to other traffickers. Victims may originate from abroad or within the United States and may be transported by air, sea and/or land domestically or internationally.

Exploitation: During this stage, traffickers profit from exploiting victims through forced labor, sexual exploitation, involuntary participation in crimes or other activity. Businesses in the service and manual labor industries (e.g., massage parlors, restaurants, farms, construction companies, domestic services) have been frequently used to exploit trafficked individuals.[3] In contrast to the one-time illicit proceeds of human smuggling, this final phase of human trafficking may generate ongoing criminal proceeds.

How to Identify Human Smuggling and Human Trafficking Transactions

To help identify and report transactions possibly associated with human smuggling and human trafficking, FinCEN has identified a number of red flags (see Appendices A and B) that financial institutions may consider incorporating into their monitoring programs. In applying these red flags, financial institutions are advised that no single transactional red flag is a clear indicator of human smuggling or trafficking-related activity. Accordingly, financial institutions should consider additional factors, such as a customer's expected financial activity, when determining whether transactions may be associated with human trafficking.

The red flags described in Appendices A and B may be associated with one or more of the stages of human smuggling or trafficking described above and may be considered by all financial institutions. Some red flags may be common to several types of financial institutions (e.g., banks, money transmitters, credit unions) while other red flags may be unique to a specific type of financial institution. Appendices A and B describe the human smuggling/trafficking stages and/or types of financial institutions most closely associated with each red flag.

In order to more effectively evaluate transactional activity, financial institutions may consider reviewing transactions at the relationship level rather than at the account level. Relationship level reviews allow financial institutions to analyze a customer's transactions across multiple accounts instead of reviewing transactions that are conducted solely through one account. This approach may also be applied when monitoring for any type of suspicious activity to offer financial institutions a more comprehensive perspective on the customer's behavior and activity.

Finally, direct interactions by branch or floor personnel with customers during the course of daily transactions can also alert financial institutions to human smuggling or trafficking-related activity. In many cases, smugglers and traffickers and/or their victims may hold accounts or receive services from financial institutions. Observations made by branch or

floor personnel can lead to the identification of anomalous activity that could alert a financial institution to initiate a review of a customer's transactions.

FinCEN Guidance to Financial Institutions

Due to some similarities with legitimate financial activities, financial institutions may consider evaluating indicators of potential human smuggling or trafficking activity in combination with other red flags and factors, such as expected transaction activity, before making determinations of suspiciousness. No one transaction or red flag by itself is a clear indicator of human smuggling or trafficking. Additionally, in making a determination of suspiciousness, financial institutions are encouraged to use previous FinCEN advisories and guidance as a reference when evaluating potential suspicious activity. For instance, in May 2014 FinCEN published an advisory on the use and structure of funnel accounts,[4] one of the red flags identified in Appendices A and B of this advisory. Financial institutions may consider incorporating the guidance outlined in this advisory in a manner that is commensurate with their risk profile and business model.

In evaluating whether certain transactions are suspicious and/or related to human smuggling or trafficking, financial institutions are encouraged to share information with one another, as appropriate, under Section 314(b) of the USA PATRIOT Act.[5] Section 314(b) establishes a voluntary information sharing mechanism allowing financial institutions to share information with one another regarding possible terrorist activity or money laundering and provides financial institutions with the benefit of a safe harbor from liability that might not otherwise exist with respect to the sharing of such information.[6] Thus, suspected money laundering involving the proceeds of human smuggling or human trafficking activity could be shared amongst financial institutions under Section 314(b).

Suspicious Activity Reporting

SARs continue to be a valuable avenue for financial institutions to report suspected human smuggling or trafficking. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report.

To assist law enforcement in targeting instances of human smuggling and trafficking, FinCEN requests that financial institutions include one or both of the below key term(s) in the Narrative and the Suspicious Activity Information:[7]

"ADVISORY HUMAN SMUGGLING" and/or "ADVISORY HUMAN TRAFFICKING"

Financial institutions should include one or both terms to the extent that financial institutions are able to distinguish between human smuggling and human trafficking. The narrative should also include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious. It is important to note that a potential victim of human smuggling or trafficking should not be reported as the subject of the

© gettechnical inc 2021

SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

Questions or comments regarding the contents of this or any other advisories should be addressed to the FinCEN Resource Center at (800) 767-2825 or (703) 905-3591. *Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).* The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

[1]*See,* 8 U.S.C. § 1324.

[2]*See* generally, 18 U.S.C. §§ 1581, 1584, 1589, 1590, 1591, 24121, 2422, 2423 and 2425, The Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. No. 106-386), applicable State laws and the President's Interagency Task Force — Progress in Combating Trafficking in Persons: The U.S. Government Response to Modern Slavery .

[3]To view the industry sectors particularly vulnerable to human trafficking, please see the U.S. Department of State Trafficking in Persons Annual Report and the July 2011 FATF Report: Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants .

[4]*See*, FinCEN (May, 2014) Advisory FIN-2014-A005 for a detailed description of funnel accounts.

[5]Pub. L. No. 107-56, § 314(b). See also, 31 CFR 1010.540.

[6]For further guidance related to the 314(b) Program, please see FinCEN's Section 314(b) Fact Sheet and FIN-2009-G002 (June, 2009), Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act.

[7]Financial institutions may include any relevant key terms in the "Other" fields of items 29 through 38, as applicable, of Part II (Suspicious Activity Information) of the SAR.

© gettechnical inc 2021

APPENDIX A

Human Smuggling Red Flags

Financial institutions may choose to use this appendix as a handout for their investigations staff and/or branch personnel. No one transaction or red flag by itself is a clear indicator of human smuggling; accordingly, financial institutions may consider applying these red flags in combination with other factors, such as a customer's profile and expected transaction activity.

Transactional and Customer Red Flags	Who would most likely see the Red Flag?
Multiple wire transfers, generally kept below the $3,000 reporting threshold, sent from various locations across the United States to a common beneficiary located in a U.S or Mexican city along the Southwest Border.[1]	Who: Banks/Credit Unions Money transmitters
Multiple wire transfers conducted at different branches of a financial institution to or from U.S or Mexican cities along the Southwest Border on the same day or on consecutive days.	Who: Banks/Credit Unions Money Transmitters/Prepaid Card Providers
Money flows that do not fit common remittance patterns: • Wire transfers that originate from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) are directed to beneficiaries located in a U.S or Mexican city along the Southwest Border. • Beneficiaries receiving wire transfers from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) who are not nationals of those countries.	Who: Banks/Credit Unions Money transmitters
Unusual currency deposits into U.S. financial institutions, followed by wire transfers to countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) in a manner that is inconsistent with expected customer activity. This may include sudden increases in cash deposits, rapid turnover of funds and large volumes of cash deposits with unknown sources of funds.	Who: Banks/Credit Unions Money transmitters

© gettechnical inc 2021

Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary, who may be located in a U.S or Mexican city along the Southwest Border. These wire senders may also use similar transactional information including but not limited to common amounts, addresses and phone numbers. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.	Who: Banks/Credit Unions Money transmitters
A customer's account appears to function as a funnel account[2], where cash deposits (often kept below the $10,000 reporting threshold) occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.	Who: Banks/Credit Unions
Checks deposited from a possible funnel account appear to be pre-signed, bearing different handwriting in the signature and payee fields.[3]	Who: Banks/Credit Unions
Frequent exchange of small-denomination for larger denomination bills by a customer who is not in a cash intensive industry. This type of activity may occur as smugglers ready proceeds for bulk cash shipments. [4]	Who: Banks/Credit Unions Casinos
When customer accounts near the Southwest Border are closed due to suspicious activity, new customers may begin transacting on behalf of those customers whose accounts have been closed. This may be done as a means to continue illicit activities. In this case, new accounts often reflect activity similar to that of the closed accounts where transactions may be frequently-occurring, currency-intensive and involve individuals that used to receive/send funds from/to accounts previously-closed due to suspicious activity.	Who: Banks/Credit Unions
Unexplained/unjustified lifestyle incommensurate with employment or business line. Profits/deposits significantly greater than that of peers in similar professions/business lines.	Who: Banks/Credit Unions Casinos/Money Transmitters/Check Cashers/Prepaid Card Providers
Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business. Extensive use of cash to purchase assets and to conduct transactions.	Who: Banks/Credit Unions Money Transmitters/Check Cashers

[1]The Southwest Border is generally described as the U.S. - Mexico land border.

© gettechnical inc 2021

[2]*See*, FinCEN (May, 2014) Advisory FIN-2014-A005 for a detailed description of funnel accounts.

[3]*See*, FinCEN (May, 2014) Advisory FIN-2014-A005 for a detailed description of funnel accounts.

[4]*See*, FinCEN (April, 2006) Advisory FIN-2006-A003 for a detailed description of repatriation of currency smuggled into Mexico from the United States.

© gettechnical inc 2021

APPENDIX B

Human Trafficking Red Flags

Financial institutions may choose to use this appendix as a handout for their investigations staff and/or branch personnel. No one transaction or red flag by itself is a clear indicator of human trafficking; accordingly, financial institutions may consider applying these red flags in combination with other factors, such as a customer's profile and expected transaction activity.

Transactional Red Flags: Behaviors observed as part of account activity	Who would most likely see the Red Flag? When most likely to see the Red Flag?
A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, social security contributions). Payroll costs can be non-existent or extremely low for the size of the customer's alleged operations, workforce and/or business line/model. When: Exploitation stage	Who: Banks/Credit Unions
Substantial deductions to wages. To the extent a financial institution is able to observe, a customer with a business may deduct large amounts from the wages of its employees alleging extensive charges (e.g., housing and food costs), where the employees only receive a small fraction of their wages; this may occur before or after the payment of wages. When: Exploitation stage	Who: Banks/Credit Unions Check Cashers/Prepaid Card Provider
Cashing of payroll checks where the majority of the funds are kept by the employer or are deposited back into the employer's account. This activity may be detected by those financial institutions that have access to paystubs and other payroll records. When: Exploitation stage	Who: Banks/Credit Unions Check Cashers/Prepaid Card Provider/Money Transmitters
The following two red flags may signal anomalous customer activity; however, they should be applied in tandem with other indicators when determining whether transactions are linked to human trafficking. Transactional activity (credits and/or debits) inconsistent with a customer's alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose.	Who: Banks/Credit Unions Check Cashers/Prepaid Card Provider/Money Transmitters/Casinos

© gettechnical inc 2021

Cash deposits or wire transfers are kept below $3,000 or $10,000 in apparent efforts to avoid record keeping requirements or the filing of Currency Transaction Reports (CTRs), respectively.	
When: Recruitment, Transportation and Exploitation stages	
Frequent outbound wire transfers, with no business or apparent lawful purpose, directed to countries at higher risk for human trafficking [1] or to countries that are inconsistent with the customer's expected activity.	Who: Banks/Credit Unions Money Transmitters
When: Recruitment, Transportation and Exploitation stages	
A customer's account appears to function as a *funnel account*,[2] where cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.	Who: Banks/Credit Unions
When: Exploitation stage	
Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary. These wire senders may also use similar transactional information including but not limited to a common address and phone number. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.	Who: Banks/Credit Unions Money Transmitters
When: Exploitation stage	
Transactions conducted by individuals, escorted by a third party (e.g., under the pretext of requiring an interpreter), to transfer funds (that may seem to be their salaries) to other countries.	Who: Banks/Credit Unions Money Transmitters/Check Cashers
When: Exploitation stage	
Frequent payments to online escort services for advertising, including small posting fees to companies of online classifieds as well as more expensive, higher-end advertising and website hosting companies.	Who: Banks/Credit Unions Money Transmitters/Prepaid Card Providers
When: Exploitation stage	
Frequent transactions, inconsistent with expected activity and/or line of business, carried out by a business customer in apparent efforts to provide sustenance to individuals (e.g., payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food).	Who: Banks/Credit Unions Money Transmitters/Prepaid Card Providers
When: Transportation and Exploitation stages	
Payments to employment or student recruitment agencies that are not licensed/registered or that have labor violations.	Who: Banks/Credit Unions

© gettechnical inc 2021

	Money Transmitters/Prepaid Card Providers/Check Cashers
When: Recruitment, Transportation and Exploitation stages	
Customer Interaction Red Flags: Behaviors observed while interacting with the public	
A customer establishes an account or visits a branch to conduct transactions while always escorted by a third party (e.g., under the pretext of requiring an interpreter). Correspondingly, the third party escorting the customer may always have possession of the customer's ID.	Who: Banks/Credit Unions Money Transmitters/Check Cashers
When: Exploitation stage	
Common signer(s)/custodian(s) in apparently unrelated business and/or personal accounts. Similarly, common information (e.g., address, phone number, employment information) used to open multiple accounts in different names.	Who: Banks/Credit Unions
When: Exploitation stage	
Accounts of foreign workers or students where the employer or employment agency serves as a custodian.	Who: Banks/Credit Unions
When: Exploitation stage	
Unexplained/unjustified lifestyle incommensurate with employment or business line. Profits/deposits significantly greater than that of peers in similar professions/business lines.	Who: Banks/Credit Unions Casinos/Money Transmitters/Check Cashers/Prepaid Card Provider
When: Recruitment, Transportation and Exploitation stages	
Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business. Extensive use of cash to purchase assets and to conduct transactions.	Who: Banks/Credit Unions Money Transmitters/Check Cashers
When: Recruitment, Transportation and Exploitation stages	

[1] To view the countries of origin, transit and destination of human trafficking victims, please refer to the U.S. Department of State Trafficking in Persons Annual Report and the July 2011 FATF Report: Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants .

[2]*See, FinCEN (May, 2014) Advisory FIN-2014-A005 for a detailed description of funnel accounts.*

© gettechnical inc 2021

FIN-2014-A005
May 28, 2014

Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML

Restrictions on USD cash transactions in Mexico may have led criminal actors to use additional schemes, such as using "funnel accounts" in conjunction with trade-based money laundering, to launder illicit proceeds

The Financial Crimes Enforcement Network (FinCEN) is issuing this update to advise financial institutions on the increased use of funnel accounts as part of trade-based money laundering conducted by criminal actors following the restrictions on U.S. currency transactions in Mexico. This Advisory provides "red flags" that may assist financial institutions identify and report suspicious funnel account activity.

Funnel Account: *An individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals*

Background

In June 2010, the Mexican government announced regulations limiting deposits of U.S. cash in Mexican banks.[1] Several months later, the Mexican government expanded the restrictions to include cash deposits made at exchange houses (casas de cambio) and brokerages (casas de bolsa). In 2011 and 2012, FinCEN issued two advisories that detailed the rise of funnel account use (also known as interstate or out-of-state funnel account activity) as a technique employed by individuals seeking to move illicit proceeds following the currency restrictions.[2] Law enforcement information and Suspicious Activity Reports (SARs) now show that Mexico- related criminal organizations: (i) continue to employ funnel accounts to move illicit proceeds and (ii) are using funnel accounts to finance the purchase of goods as part of Trade- Based Money Laundering (TBML) activity.

In some instances, multiple funnel accounts have been observed to transfer funds into a single consolidated account from where the funds are subsequently withdrawn. Criminal organizations use wires and checks issued from funnel accounts to move illicit narcotics proceeds to the accounts of businesses offering trade goods and services as part of trade-based money laundering as further described below.

© gettechnical inc 2021

Schemes such as the use of funnel accounts and TBML are a money laundering concern for both the U.S. and Mexican governments.

Funnel Accounts and Trade-Based Money Laundering

Typical steps of funnel account activity in conjunction with trade-based money laundering include:

(I) A U.S. or foreign business owner or other individual, colluding with representatives of a criminal organization, opens an account at banks or credit unions whose accounts can readily receive cash deposits in multiple states through their own branches or through shared branches.[3]

(II) Multiple individuals acting on behalf of representatives of the criminal organization deposit the cash proceeds of narcotics sales into this account at different bank or credit union branches, often in multiple states geographically distant from the branch in which the account was opened or domiciled. The deposits are kept below $10,000 in order for transactors to avoid identification and record keeping requirements.

(III) After a number of deposits have been credited to the account, an intermediary will initiate wire transfers (or issue checks) from the funnel account to a U.S. or foreign-based business for the purchase of goods that are then shipped to foreign countries for sale.

(IV) Once the purchased goods arrive at the destination country, they are sold and the sale proceeds, in the destination country's currency, are transferred to the drug trafficking or money laundering organization to provide the criminal actors with funds that have been laundered through TBML.[4]

When the goods in this scheme are sold in Mexico, a drug trafficking organization or its intermediary, often termed a "money broker" or "peso broker,"[5] will contract with a U.S. or Mexican business owner to open a funnel account at banks or credit unions whose accounts can readily receive cash deposits in multiple states. The peso broker subsequently directs the deposit of narcotics proceeds into the funnel account and makes payments from this account for the purchase of U.S. and foreign goods. These goods are then shipped to Mexican businesses where they are sold for pesos. In essence, the drug trafficking organization has exchanged the U.S. dollar cash proceeds in the United States for Mexican pesos in Mexico through the use of a funnel account and TBML. The criminal actors can both repatriate and give a plausible source to the proceeds of illicit activity obtained in the United States through apparently legitimate business transactions.

Funnel Accounts and Trade-Based Money Laundering Red Flags

A funnel account associated with TBML might manifest one or more of the following red flags:

© gettechnical inc 2021

- An account opened in one state (typically along the Southwest border) receives multiple cash deposits of less than $10,000 by unidentified persons at branches outside of the geographic region where the account is domiciled. The accounts receiving the out-of-state deposits can be either individual or business accounts.

- In the case of a business account, the deposits take place in a different geographic region from where the business operates.[6] For example, the account of a produce company operating locally in Southern California receives small cash deposits, below the currency reporting threshold, at bank branches in Chicago, Indianapolis, and Minneapolis.

- If questioned, the individuals opening or making deposits to funnel accounts may have no detailed knowledge about the stated business activity of the account, the account holder (in the case of a depositor), or the source of the cash. This is because criminal organizations sometimes pay individuals outside their organization, such as students, itinerant workers, or the un/ under-employed to open or carry out funnel account transactions.

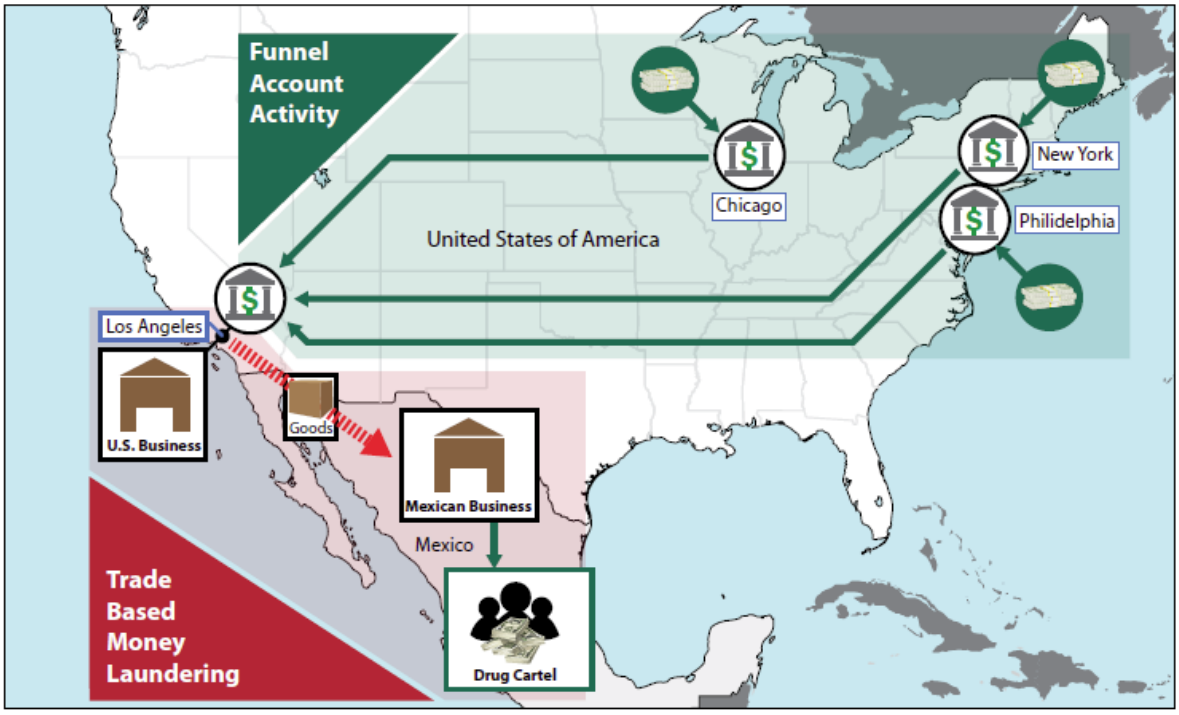
- In the case of a business account receiving out-of-state deposits, the debits do not appear to be related to the stated business activity of the account holder. For example, checks drawn on the account of a produce company are made payable to a leather goods business, or funds are wired from the produce company's account to a textile manufacturer in China.[7]

- Checks issued from an account that receives out-of-state cash deposits appear to have different handwriting on the payee and amount lines than the signature line. This may indicate that (i) the checks, originally issued to the account holder, have been pre-signed but the payee and amount lines have been left blank, then (ii) the checks were handed over to a criminal organization, which then (iii) used the checks to pay U.S. or foreign parties by populating the payee and amount fields.

- Wire transfers or checks issued from a funnel account are deposited into, or cleared through, the U.S. correspondent account of a Mexican bank. In addition to exhibiting funnel account activity, in some cases, checks issued from the U.S. account name a Mexican bank as payee and the checks are either deposited into the Mexican bank's U.S. correspondent account or are cleared through said correspondent account by cash letter.

© gettechnical inc 2021

Funnel Account Activity and Trade Based Money Laundering



© gettechnical inc 2021

FINCEN FIN-2012-A009: SUSPICIOUS ACTIVITY RELATED TO MORTGAGE LOAN FRAUD (8/16/2012)

FIN-2012-A009
Issued Date: August 16, 2012
Subject: Suspicious Activity Related to Mortgage Loan Fraud

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to highlight activity related to mortgage loan fraud so that financial institutions may better assist law enforcement when filing Suspicious Activity Reports (SARs). This Advisory, which consolidates certain information from previously issued FinCEN reports, contains examples of common fraud schemes and potential "red flags" for activity related to mortgage loan fraud. Using this additional information, the vigilance of financial institutions, together with law enforcement efforts against illicit mortgage-related activities, will help protect financial institutions and their customers from financial loss, and support the housing markets and the U.S. financial system as a whole.

This Advisory supports the efforts of the Financial Fraud Enforcement Task Force (FFETF),[1] the U.S. Department of the Treasury's broader initiatives to ensure that U.S. financial institutions are not used as conduits for illicit activity, and a FinCEN and U.S. Department of Housing and Urban Development (HUD) OIG mortgage fraud initiative.

Types of Mortgage Loan Fraud Identified by Law Enforcement

The following list identifies types of mortgage loan fraud, which are primarily based upon schemes and scams frequently reported or described in SARs or identified by our law enforcement and regulatory partners. This information is intended to assist financial institutions in identifying when illicit activities occur in connection with mortgage loan transactions.

Occupancy fraud: Occurs when borrowers, to obtain favorable loan terms, claim that subject properties will be their primary residences instead of vacation homes or investment properties. It also occurs when subjects apply for loans for properties that others, such as family members, will actually occupy.

Income fraud: Includes both overstating income to qualify for larger mortgages and understating income to qualify for hardship concessions and modifications.

Appraisal fraud: Includes both overstating home value to obtain more money from a sale of property or cash-out refinancing, and understating home value in connection with a plan to purchase a property at a discount to market value.

Employment fraud: Includes misrepresenting whether, where, and for how long borrowers have been employed; whether borrowers are unemployed or collecting unemployment benefits; and whether borrowers are independent contractors or business owners.

© gettechnical inc 2021

Liability fraud: Occurs when borrowers fail to list significant financial liabilities, such as other mortgages, car loans, or student loans, on mortgage loan applications. Without complete liability information, lenders cannot accurately assess borrowers' ability to repay debts.

Debt elimination schemes:[2] Involves the use of fake legal documents and alternative payment methods to argue that existing mortgage obligations are invalid or illegal, or to purport to extinguish mortgage balances. Individuals orchestrating debt elimination schemes typically charge borrowers a fee for these debt elimination "services."

Foreclosure rescue scams:[3] Targets financially distressed homeowners with fraudulent offers of services or advice aimed at stopping or delaying the foreclosure process. Some of these scams require homeowners to transfer title - or make monthly mortgage payments - to the purported "rescuer," rather than the real holder of the mortgage. Some foreclosure rescue scams require homeowners to pay fees before receiving "services," and are known as "advance fee" schemes.

Social Security Number (SSN) Fraud and other Identify Theft:[4] Includes the use of an SSN or other government identification card or number that belongs to someone other than the applicant in a loan application. Identity Theft includes broader use of another's identity or identifiers (beyond an SSN) to obtain a mortgage or perpetrate a "fraud for profit" scheme.

Home Equity Conversion Mortgage (HECM):[5] Financial institutions need be aware of illegal "reverse mortgage" schemes, which targets seniors who own a home or who are coerced into taking title to a home, for the purpose of stealing or otherwise acquiring some or all of the funds the senior receives from a government HECM program. HECM fraud may involve other frauds, including appraisal fraud (to increase the stated value of the home), investment fraud to acquire the HECM funds from the senior under the guise of future profits for the senior, and identify theft to acquire HECM funds without the knowledge of the senior who owns the property.

Possible Red Flag Indicators of Mortgage Loan Fraud

The following highlights potential red flag indicators of illicit activity related to mortgage fraud. These only indicate possible signs of fraudulent activity; they do not constitute an exhaustive list of common fraud schemes. No single red flag will be definitive proof of such activity and many apply to multiple fraud schemes. Instead, it is important to view any red flag(s) in the context of other indicators and facts, such as the specific role of the financial institution within mortgage loan-related transaction(s), as well as the institution's knowledge of any associated fraud schemes. The presence of any of these red flags in a given transaction or business arrangement may indicate a need for further due diligence and a decision whether to file a SAR.

- Borrower/buyer submits invalid documents in order to cancel his or her mortgage obligations or to pay off his or her loan balance(s).
- Same notary public and/or other "authorized representative" preparing, signing, and sending packages of nearly identical debt elimination documents for multiple borrowers with outstanding mortgage balances.
- Same notary public and/or other "authorized representative" working with and/or receiving payments from unusually large numbers of borrowers.
- Falsification of certified checks, cashier's checks or "non-cash item checks" drawn against a borrower/buyer's account, rather than from the account of a financial institution.
- Borrower/buyer applies for a loan for a "primary residence " but does not reside in the new primary residence as indicated on the loan application; other individuals occupy the

© gettechnical inc 2021

borrower/buyer's new primary residence indicating the property is being used as a secondary residence or income-generating property.

- Borrower/buyer of a younger age purchases his or her "primary residence" in a senior citizen residential development.
- Borrower/buyer requests refinancing for "primary residence" when public and personal documents indicate that the borrower/buyer resides somewhere other than the address on the loan application.
- Language included in a short sale contract indicates the property could be resold promptly. This possibly illegal "flipping" may occur regardless of whether the Federal Housing Administration (FHA) has re-enacted or waived its arms-length resale regulations to FHA buyers.
- Low appraisal values, non-arms length relationships between short sale buyers and sellers, or previous fraudulent sale attempts in short-sale transactions,.
- Agent of the buyer and/or seller in mortgage transaction is unlicensed.
- Past misrepresentations made by borrower/buyer in attempts to secure funding, property, refinance, and/or shorts sales.
- Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information.
- Apparent resubmission of rejected loan application with key borrower/buyer details changed or modified from individual borrower to company/corporation. This activity may identify the same person attempting to secure a loan fraudulently through a straw-borrower or non-existent person.
- Borrower/buyer attempts to structure currency deposits/withdrawals, or otherwise to hide or disguise the true value of assets, in order to qualify for loan modification programs intended for those homeowners in financial distress.
- Request from third party affiliates on behalf of distressed homeowners to pay fees in advance of the homeowner receiving mortgage counseling, foreclosure avoidance, a loan modification, or other related services.
- Third party solicitation of distressed homeowners for purported mortgage counseling, foreclosure avoidance, loan modification, or other related services. These third parties may also claim to be associated with legitimate mortgage lenders, the U.S. government, or a U.S. government program.[6]

Suspicious Activity Reporting

If a financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity or an attempt to disguise funds derived from illegal activity, is designed to evade regulations promulgated under the Bank Secrecy Act, or lacks a business or apparent lawful purpose, the financial institution may be required to file a SAR.[7] When completing SARs on suspected mortgage loan fraud, financial institutions should indicate the type of mortgage loan fraud by entering the appropriate code in the FinCEN SAR and provide a detailed description in the SAR narrative. For activity that does not have a corresponding code, financial institutions should identify "Other" and describe the activity in the narrative.[8]

Financial institutions, when filing a SAR, are also requested, where available, to include in the narrative portion, the Conference of State Bank Supervisors' (CSBS) National Mortgage Licensing System and Registry (NMLS) assigned "NMLS Unique Identifier." As required by Section 1503 of the Secure and Fair Enforcement for Mortgage Licensing Act of 2008 (SAFE

© gettechnical inc 2021

Act), a NMLS unique identifier is permanently assigned to each state-licensed or federally registered mortgage loan originator (MLO), as well as each company, branch, and control person that maintains a single account in NMLS. The value of the NMLS Unique Identifier has been recognized by the Federal Housing Finance Agency (FHFA) and HUD. Both federal agencies require that any loan purchased or securitized by Fannie Mae and Freddie Mac, or submitted for insurance by the FHA, must include the NMLS Unique Identifier for the company and individual MLO that originated the mortgage loan.

Questions or comments regarding the contents of this advisory or the June 2010 Advisory should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. *Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).* The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

[1]For more information on the FFETF and its current initiatives, please visit https://www.fincen.gov/financial-fraud-enforcement-task-force-ffetf..

[2]For additional information pertaining to schemes of this type, please see the June 2010 Advisory, available at: https://www.fincen.gov/sites/default/files/shared/fin-2010-a006.pdf.

[3]For additional information pertaining to foreclosure rescue fraud schemes, please see the April 2009 Advisory, available at: https://www.fincen.gov/sites/default/files/shared/fin-2009-a001.pdf.

[4]For additional information and resources from FinCEN and links to other governmental efforts to combat identity theft, please visit FinCEN's website at: https://www.fincen.gov/resources-victims.

[5]For additional information pertaining to Home Equity Conversion Mortgage (HECM) fraud schemes, please see the April 2010 Advisory, available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a005.

[6]For additional information pertaining to schemes of this type, please see the June 2010 Advisory, available at: https://www.fincen.gov/sites/default/files/shared/fin-2010-a006.pdf.

[7]See, e.g., 31 CFR § 1020.320 and 31 CFR § 1029.320

[8]For additional assistance on key terms related to types of real estate fraud, please see the Suspicious Activity Report (SAR) Advisory Key Terms Guidance, available at: https://www.fincen.gov/suspicious-activity-report-sar-advisory-key-terms

© gettechnical inc 2021

FINCEN GUIDANCE FIN-2012-G002 : FILING FINCEN'S NEW CURRENCY TRANSACTION REPORT AND SUSPICIOUS ACTIVITY REPORT (3/29/12)

Department of the Treasury
Financial Crimes Enforcement Network

Guidance

FIN-2012-G002
Issued: March 29, 2012

Subject: Filing FinCEN's new Currency Transaction Report and Suspicious Activity Report
Today, the Financial Crimes Enforcement Network (FinCEN) began to accept the new Currency Transaction Report (CTR) and Suspicious Activity Report (SAR) into FinCEN's BSA E-Filing System. Together, these two new reports will replace FinCEN Form 104 (CTR), FinCEN Form 103 (CTR by Casinos), and all of the industry-specific SARs (TD F 90-22.47, FinCEN Form 101, FinCEN Form 102, and FinCEN Form 109), hereinafter referred to as "legacy reports."
While the new CTR and SAR forms do not create any new obligations or otherwise change existing statutory and regulatory expectations of financial institutions, this guidance is intended to assist institutions filing the new reports.

Timeline and Filing Method

FinCEN is now accepting the new CTR and SAR filings through the BSA E-Filing System. The BSA E-Filing System will continue to accept submissions of the legacy reports until March 31, 2013. Accordingly, until such time, financial institutions may choose to electronically file either the legacy or new reports, or any combination thereof.
In a separate action, FinCEN has mandated electronic filing of most reports through the BSA E-Filing System, beginning July 1, 2012.[1] While FinCEN strongly recommends that financial institutions begin to file electronically before the mandate takes effect, financial institutions may continue to file, via paper, the most currently available versions of the legacy reports before July 1, 2012.[2] The new CTR and SAR reports may only be submitted electronically.

[1] *See* Agency Information Collection and Reporting Activities; Electronic Filing of Bank Secrecy Act (BSA) Reports, Final Notice, 77 Fed. Reg. 12367 (2012), at http://www.gpo.gov/fdsys/pkg/FR-2012-02-29/pdf/2012-4756.pdf.
[2] *See* Important Notice for Financial Institutions, FinCEN Extends Deadline for Adopting New CTR and SAR (2011), at http://www.fincen.gov/whatsnew/pdf/20111220.pdf. The following are the currently available forms: FinCEN 101 (SAR-SF), dated March 2011, at http://www.fincen.gov/forms/files/fin101_sar-sf.pdf; FinCEN 102 (SAR-C), dated March 2011, at http://www.fincen.gov/forms/files/fin102_sar-c.pdf; FinCEN 103 (CTR-C),

© gettechnical inc 2021

Background

FinCEN's new CTR and SAR were developed through dialogue with our federal law enforcement and regulatory partners. The modernized information technology (IT) system is driven by the data collection instead of form design. The modernized IT system incorporates additional data elements for certain fields on the new CTR and SAR. Some of the data elements will trigger third-party data enhancements after the new reports are received by FinCEN, such as postal geographic validation of entries in address fields, which will help ensure consistency in reporting and allow users of FinCEN's modernized IT system to benefit from the enhanced information. All of these updates to the IT system will allow more advanced and sophisticated querying for our law enforcement and regulatory partners.

As part of the consultation process, FinCEN also requested public comments on the proposed report fields.[3] Comments received regarding the development of the new modernized IT system have been incorporated to the extent possible. For more information on comments and dispositions, please see http://www.fincen.gov/forms/bsa_forms/.

This guidance clarifies certain inquiries posed by industry regarding the new reports. FinCEN recognizes that it may need to develop further guidance regarding the filing of the new reports to address additional questions. FinCEN will develop any future guidance through continued dialogue with the industry, law enforcement and regulatory communities. In addition, FinCEN will continue working with supervisory regulatory authorities as part of its ongoing efforts to promote consistent examination of these filing requirements.

On September 8, 2011, FinCEN released electronic filing requirements for the new CTR and electronic filing requirements for the new SAR. These technical specifications were released to allow the development of batch files of the new CTR and SAR for upload or transmission to the BSA E-Filing System.[4] On February 17, 2012, FinCEN announced the availability of the BSA E-Filing System's User Test System Website to allow for testing submissions of batch and computer-to-computer filings of the new CTR and SAR.[5] Additionally, the site offered a preview of the PDF versions of these new reports, for discrete filing. In the near future, FinCEN will be announcing additional educational webinars on the new reports to ensure all financial institutions are prepared to utilize the new reports no later than March 31, 2013.

Guidance

Characterizations of Suspicious Activity

---

dated March 2011, at http://www.fincen.gov/forms/files/fin103_ctrc.pdf; FinCEN 104 (CTR), dated March 2011, at http://www.fincen.gov/forms/files/fin104_ctr.pdf; TD F 90-22.47 (SAR-DI), dated March 2011, at http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf; and FinCEN 109 (SAR-MSB), dated March 2011, at http://www.fincen.gov/forms/files/fin109_sarmsb.pdf .

[3] *See* Proposed Collection; Comment Request; Bank Secrecy Act Unified Currency Transaction Report Proposed Data Fields, 76 Fed. Reg. 4747 (2011), at http://edocket.access.gpo.gov/2011/pdf/2011-1587.pdf; *see also* Proposed Collection; Comment Request; Bank Secrecy Act Suspicious Activity Report Database Proposed Data Fields, 75 Fed. Reg. 63545 (2010), at http://edocket.access.gpo.gov/2010/pdf/2010-26038.pdf.

[4] *See* Important Notices to E-Filers: FinCEN Releases Technical E-Filing Specifications for New CTR and SAR (2011), Announces Informational Webinar, at http://www.fincen.gov/news_room/nr/pdf/20110902.pdf.

[5] *See* Important Notice for Financial Institutions, FinCEN Releases Test Site for the New CTR and SAR (2012), at http://www.fincen.gov/news_room/nr/pdf/20120217.pdf.

© gettechnical inc 2021

FinCEN's new CTR and SAR are designed to accommodate all the different types of industries that will file these reports. As such, the new SAR contains certain sections of suspicious activity characterizations, which will generally be most relevant to a specific industry. When the filing institution's industry is selected, in the discrete version of the report, those sections specific to other industries will automatically be noted as not applicable, by being grayed out.[6]

In addition, the new CTR and SAR include a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. The decision to include these additional data elements in the new SAR arose from extensive discussions with law enforcement officials. It was determined that the inclusion of such elements would facilitate more effective use of the information collected in the reports. FinCEN acknowledges that the expansion of these characterizations may create the need for clarification on how to select among the choices provided to depict the activity, as well as how to describe this information in Part V, the narrative.

FinCEN does not intend the issuance of the new SAR to create new obligations for filing institutions, or to change existing requirements or expectations. When evaluating suspicious activity and completing a SAR, institutions should report the characteristics of the suspicious activity and types of financial services that best apply, based on information that readily comes available during the course of their case reviews. FinCEN is making available the additional and more specific data elements (i.e., characterizations of suspicious activity and types of financial services) as a more efficient way to bring information about suspicious activity to FinCEN's and law enforcement's attention. Other than the Critical Fields (see the below section entitled "Critical Fields") filers should not consider the presence of the new and expanded lists of data elements as requiring them to determine as part of their reviews whether any and/or all apply to the matter being reported. As before, financial institutions should report the information that they know, or that otherwise arises, as part of their case reviews. Moreover, the addition of the new and expanded data elements does not create an expectation that financial institutions will revise internal programs, or develop new programs, to capture information that reflects the expanded lists. FinCEN continues to reiterate that institutions are not responsible for investigating the underlying suspected (or alleged) crime; investigations remain the responsibility of law enforcement. Institutions are responsible for reporting the information they know at the time they conclude that suspicious activity is present.

Critical Fields

Certain fields in the new CTR and SAR are marked as "critical" for technical filing purposes;[7] this means that the BSA E-Filing System will not accept filings in which these fields are left blank. For these items, the filing institution must either provide the requested information or affirmatively check the "unknown" (Unk.) box that is provided with each critical field. This unknown box will thus supersede FinCEN's previous guidance where we have requested that filers input "N/A" or "XX" in certain fields. For those fields that are not marked as "critical" for technical filing purposes,[7] the BSA

[6] As an example, if the filer is a broker-dealer, then insurance and casino selections may be grayed out; if the filer is a depository institution, then casino and the broker-dealer selections are grayed out. The full implementation of this capability is still being developed. Filers may choose to enable and use these fields, as necessary, for example, in reporting activity that involves affiliated institutions across industry sectors. Institutions that batch file their reports may not have this feature, based on software design.

[7] Critical fields are denoted with an "*." This differentiation between critical and noncritical items is consistent with the most current versions of certain legacy reports. *See, e.g.,* FinCEN Form 101, Suspicious Activity Report by the Securities and Futures Industries, and FinCEN Form 103, Currency Transaction Report by Casinos. This differentiation is also consistent with how the BSA E-Filing System currently accepts the legacy reports, requiring

© gettechnical inc 2021

E-Filing System will accept reports, in which these fields have been left blank. FinCEN expects, however, that financial institutions will provide the most complete filing information available within each report consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.

SAR Narrative

The SAR Narrative will remain a critical component of the SAR filing. However, with the flexibility of the suspicious activity section, it was determined that less characters may be necessary in the narrative section. Thus, the number of narrative characters has been limited to 17,000 characters (as compared to approximately 39,000 characters, in the legacy forms). However, the new SAR narrative also allows filers to include an attachment that the financial institution believes would be useful to law enforcement (see the below section entitled "Spreadsheet Attachments").

Gender Field

FinCEN has been asked for guidance on the "Gender" Field (Item 4 of Part I: Subject Information on the SAR and Item 5 of Part I Person Involved in Transaction on the CTR). Based on feedback from law enforcement officials, information related to the gender of the subject could be an important characteristic for query purposes. As stated previously, for both the critical and noncritical elements, institutions should complete those items, for which they have relevant information. However, use of this field is not mandatory, and as the instructions indicate, this does not create an obligation for a financial institution to collect gender information, either manually or through an enterprise-wide IT management system, especially when such collection would be in conflict with the financial institution's obligations under any other applicable law.

NAICS Code

FinCEN has also been asked for guidance on the use of the North American Industry Classification System (NAICS) code field (Item 7a on the SAR and Item 9a on the CTR). Law enforcement officials have indicated that the NAICS code is beneficial in CTR and SAR data; however, FinCEN emphasizes that financial institutions will continue to be expected to provide only that information, for which they have direct knowledge. Again, the issuance of the new CTR and SAR does not create any new obligation or otherwise change existing statutory and regulatory requirements for the filing institution. In addition, financial institutions are not required to become familiar with NAICS codes, as the appropriate list of codes is contained in a drop down menu that automatically populates the field. In addition, use of a NAICS code is not mandatory, and a financial institution may still provide a text response with respect to this information.

Fields Related to Internet Presence

The new SAR includes certain new elements related to the internet presence of subjects and suspicious activity, specifically the "E-mail address" and "Website (URL) address" fields within Part I: Subject Information and "IP address (if available)," in Part II: Suspicious Activity Information. These are items which many filers have previously included in the narratives of the legacy SARs in the context of describing suspicious activity. For example, to show that suspected criminal activity was being conducted from a specific internet site location. By providing a discrete space into which such information may additionally be entered, the new reports will facilitate FinCEN's and law enforcement's ability to make connections between elements reported across separate filings and external data sources. In doing so, FinCEN does not intend to create any obligation or expectation

---

that certain fields be filled in before accepting a filing.

© gettechnical inc 2021

that financial institutions would collect this information as a matter of course. The narrative section of the report may be used to provide more information as to how an internet presence relates to the suspicious activity or to provide any other relevant email or IP addresses that may pertain to non-subjects.

Spreadsheet Attachments

The new SAR will accept a single, comma separated value (CSV) attachment as part of the report. The CSV is a standard Microsoft file format that aids in reporting tabular data into a file format. This capability allows an institution to include data (such as specific financial transactions and funds transfers or other analytics), which is more readable and usable in this format than it would be if otherwise included in the narrative. Such an attachment will be considered a part of the narrative and is not considered to be a substitute for the narrative. As with other information that may be prepared in connection with the filing of a SAR, it can also be considered supporting documentation when not attached to the SAR and should be accorded confidentiality to the extent that it indicates the existence of a SAR.
Tool Completion

Financial institutions will note that the line item instructions for the new SAR from Part I to Part V differ from the order that the discrete electronic collection tool is completed. Specifically, the automated discrete collection tool begins with Part IV, Filing Institution. For the majority of SARs filed, the filing institution and the location where the suspicious activity occurred are the same. By completing Part IV first, the collection tool is able to auto populate Part III, Location Where Activity occurred, if it is the same, thereby saving the filer having to re-enter the same information again. Additionally, with the deployment of the enhanced e-filing registration process, the use of additional auto population options will be available, to further reduce manual entry of certain fields, in the electronic collection tool.

Timeframe for Filing CTRs

FinCEN announced a change in the CTR electronic filing specification for the CTR from the current 25-days to 15-days.[8] FinCEN regulations have consistently maintained a regulatory requirement that CTRs be filed within 15 days.[9] Notwithstanding this requirement, in connection with its receipt of magnetic media files initiated in late 1987, and ending in December 2008, FinCEN issued electronic specifications referencing a 25-day period, to assist institutions seeking to take advantage of this filing method via a common business practice of submitting magnetic media files on a fixed schedule. The 25-day period was implemented to account for physically transporting (shipping) the magnetic media to the processing center in Detroit, Michigan. FinCEN understands that this business practice has continued with respect to batch e-filing, particularly considering public guidance referencing the 25-day period. In light of the comments received and acknowledging that some financial institutions may need to change their business processes to become compliant with the rules, FinCEN has determined that it will temporarily maintain the 25-day compliance period referenced in its earlier specifications until March 31, 2013. This temporary extension to the filing requirements should allow sufficient time for filers to adjust submission schedules to meet established regulatory requirements.

---

[8] The FinCEN CTR filing specifications may be viewed at http://bsaefiling.fincen.treas.gov/news/FinCENCTRElectronicFilingRequirements.pdf. *See* Appendix D, page 49.
[9] 9 *See* 31 CFR 1010.306(a)(1).

© gettechnical inc 2021

FINCEN ADVISORY FIN-2011-A003 ADVISORY TO FINANCIAL INSTITUTIONS ON FILING SUSPICIOUS ACTIVITY REPORTS REGARDING ELDER FINANCIAL EXPLOITATION (2/11/11)

Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2011-A003
Issued: February 22, 2011
Subject: Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist the financial industry in reporting instances of financial exploitation of the elderly, a form of elder abuse.[10] Financial institutions can play a key role in addressing elder financial exploitation due to the nature of the client relationship. Often, financial institutions are quick to suspect elder financial exploitation based on bank personnel familiarity with their elderly customers. The valuable role financial institutions can play in alerting appropriate authorities to suspected elder financial exploitation has received increased attention at the state level; this focus is consistent with an upward trend at the federal level in Suspicious Activity Reports (SARs) describing instances of suspected elder financial exploitation.[11] Analysis of SARs reporting elder financial exploitation can provide critical information about specific frauds and potential trends, and can highlight abuses perpetrated against the elderly.

This advisory contains examples of "red flags" based on activity identified by various state and federal agencies and provides a common narrative term that will assist law enforcement in better identifying suspected cases of financial exploitation of the elderly reported in SARs.

Older Americans hold a high concentration of wealth as compared to the general population. In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical well-being, financial management, and social interaction. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

[10] Abuse and exploitation of the elderly is statutorily defined at the state level. The National Center on Elder Abuse offers the following definition of exploitation as a type of elder abuse: "the illegal taking, misuse, or concealment of funds, property, or assets of a vulnerable elder."

[11] Bank Secrecy Act data reflects increasing use of terms related to elder financial exploitation/abuse in SAR narratives.

© gettechnical inc 2021

Potential Indicators of Elder Financial Exploitation
The following red flags could indicate the existence of elder financial exploitation. This list of red flags identifies only *possible* signs of illicit activity. Financial institutions should evaluate indicators of potential financial exploitation in combination with other red flags and expected transaction activity being conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine if the activity is suspicious.
Financial institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior. In addition, financial institutions may become aware of such scams through their direct interactions with elderly customers who are being financially exploited. In many cases, branch personnel familiarity with specific victim customers may lead to identification of anomalous activity that could alert bank personnel to initiate a review of the customer activity.

• Erratic or unusual banking transactions, or changes in banking patterns:
o Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;

o Sudden Non-Sufficient Fund activity;

o Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;

o Debit transactions that are inconsistent for the elder;

o Uncharacteristic attempts to wire large sums of money;

o Closing of CDs or accounts without regard to penalties.

• Interactions with customers or caregivers:
o A caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;

o The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;

o The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;

o A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;

o The customer moves away from existing relationships and toward new associations with other "friends" or strangers;

o The elderly individual's financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual;

o The elderly customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

© gettechnical inc 2021

Suspicious Activity Reporting

SARs continue to be a valuable avenue for financial institutions to report elder financial exploitation. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Part 103 (future 31 CFR Chapter X), if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should then file a Suspicious Activity Report.[12]

In order to assist law enforcement in its effort to target instances of financial exploitation of the elderly, FinCEN requests that financial institutions select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and include the term "elder financial exploitation" in the narrative portion of all relevant SARs filed. The narrative should also include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious. It is important to note that the potential victim of elder financial exploitation *should not be reported as the subject* of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

Elder abuse, including financial exploitation, is generally reported and investigated at the local level, with Adult Protective Services, District Attorney's offices, sheriff's offices, and police departments taking key roles. We emphasize that filers should continue to report all forms of elder abuse according to institutional policies and the requirements of state and local laws and regulations, where applicable. Financial institutions may wish to consider how their AML programs can complement their policies on reporting elder financial exploitation at the local and state level.

Financial institutions with questions or comments regarding this Advisory should contact FinCEN's Regulatory Helpline at 800-949-2732.

[12] Financial institutions shall file with FinCEN to the extent and in the manner required a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a Suspicious Activity Report with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations. *See, e.g.,* 31 CFR § 103.18(a) (future 31 CFR § 1020.320(a)).

© gettechnical inc 2021

COVID

© gettechnical inc 2021

FinCEN ADVISORY

FIN-2020-A007 October 13, 2020

Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to unemployment insurance (UI) fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related UI fraud, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Financial Red Flag Indicators of Unemployment Insurance Fraud Related to COVID-19 Relief

As unemployment claims in the United States have surged due to the pandemic, U.S. law enforcement and financial institutions have detected numerous instances of COVID-19-related UI fraud. The following are representative types of this illicit activity:

- *Fictitious employer-employee fraud:* filers falsely claim they work for a legitimate company, or create a fictitious company and supply fictitious employee and wage records to apply for UI payments;
- *Employer-employee collusion fraud:* the employee receives UI payments while the employer continues to pay the employee reduced, unreported wages;
- *Misrepresentation of income fraud:* an individual returns to work and fails to report the income in order to continue receiving UI payments, or in an effort to r eceive higher UI payments, an applicant claims higher wages than he/she previously earned;

© gettechnical inc 2021

- *Insider fraud:* state employees use credentials to inappropriately access or change UI claims, resulting in the approval of unqualified applications, improper payment amounts, or movement of UI funds to accounts that are not on the application; or
- *Identity-related fraud:* filers submit applications for UI payments using stolen or fake identification information to perpetrate an account takeover.[13]

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate.

FinCEN identified the financial red flag indicators described below to alert financial institutions to fraud schemes targeting UI programs, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such fraud. Financial red flag indicators of UI fraud may include:

1. Account(s) held at the financial institution receive(s):
   a. UI payments from a state other than the state in which the customer reportedly resides or has previously worked;
   b. Multiple state UI payments within the same disbursement timeframe;
   c. UI payments in the name of a person other than the accountholder, or in the names of multiple unemployment payments recipients;
   d. UI payments and regular work-related earnings, via direct deposit or paper checks;
   e. Numerous deposits or electronic funds transfers (EFTs) that indicate they are UI payments from one or more states to persons other than the accountholder(s);
   f. A higher amount of UI payments in the same timeframe than similarly situated customers received.
2. The customer withdraws the disbursed UI funds in a lump sum by cashier's checks, by purchasing a prepaid debit card, or by transferring the funds to out-of-state accounts.
3. The customer's UI payments are quickly diverted via wire transfer to foreign accounts, particularly to accounts in countries with weak anti-money laundering controls.

[13] *See*, FinCEN Advisory, FIN-2020-A005, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020). In some situations, fraudsters use the stolen identification information to perpetrate an account takeover. For additional information on identifying account takeover activity, *see* FinCEN Advisory, FIN-2011-A016, "Account Takeover Activity," (December 19, 2011).

© gettechnical inc 2021

4. The customer receives or sends UI payments to a peer-to-peer (P2P) application or app. The funds are then wired to an overseas account, or withdrawn using a debit card, in a manner that is inconsistent with the spending patterns of similarly situated customers.
5. Individuals quickly withdraw disbursed UI funds via online bill payments addressed to an individual(s), as opposed to businesses, as payee(s), with some individual payees receiving multiple online bill paychecks over a short time period.
6. The IP address associated with logins for an account conducting suspected UI-fraud activities does not map to the general location of stated address in identity documentation for the customer or where the UI payment originated.
7. Individuals direct UI-related EFTs, or deposit UI checks into suspected shell/front company accounts, which may be indicative of money mules transferring these funds in and out of the accounts.
8. Multiple accounts receiving UI payments at one or more financial institutions are associated with the same free, web-based email account that may appear in more than one UI application.
9. A newly opened account, or an account that has been inactive for more than thirty days, starts to receive numerous UI deposits. After a financial institution suspects UI fraud and requests additional identification documentation to verify the identity(ies) of the customer(s), queried individuals provide documents that are incorrect or forged, which may be an indicator of an account takeover or identity theft.
10. After a financial institution suspects UI fraud and conducts due diligence, it determines that the customer does not have a history of living at, or being associated with, the address to which the UI check or UI debit card is sent, or within the geographical area in which the registered debit card is being used.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping unemployment insurance fraud related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative.

- FinCEN requests that financial institutions reference this advisory by including the key term "**COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

- Financial institutions also should select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. When addressing unemployment fraud in a

© gettechnical inc 2021

SAR, financial institutions should include the keywords "unemployment fraud" in SAR field 34(z).

- When filing a SAR, in addition to standard transaction data, providing the following information is highly valuable to law enforcement: relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, cyber-related information and technical indicators, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI)), phone numbers, monikers, and description and timing of suspicious electronic communications.
- Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov. To report suspected illicit activity please visit our website at https://www.fincen.gov/coronavirus, which also contains information on registering to receive FinCEN Updates.

FinCEN ADVISORY

FIN-2020-A005 July 30, 2020

Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of cybercrime and cyber-enabled crime observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related malicious cyber activity and scams, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will continue issuing COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at https://www.fincen.gov/coronavirus, which also contains information on how to register to receive FinCEN Updates.

Financial Red Flag Indicators of Cybercrime and Cyber-Enabled Crime Exploiting COVID-19

This advisory addresses the primary means by which cybercriminals and malicious state actors are increasingly exploiting the COVID-19 pandemic in cyber-enabled crime through malware and phishing schemes, extortion, business email compromise (BEC) fraud, and exploitation of remote applications, especially against financial and healthcare systems.[14]

[14] *See* Department of Justice (DOJ) Press Release, "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams," (April 22, 2020); the United Kingdom (U.K.) National Cyber Security Centre (NCSC) Press Release, "Public Urged to Flag Coronavirus Related Email Scams as Online Security Campaign

© gettechnical inc 2021

FinCEN has identified the following red flag indicators of COVID-19 cyber-enabled crimes[15]
to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic. As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of potential fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities. Given that many scammers may be directly targeting customers, financial institutions should remain on the alert for potential suspicious activities involving their customers.

Targeting and Exploitation of Remote Platforms and Processes

The significant migration toward remote access in the pandemic environment presents opportunities for criminals to exploit financial institutions' remote systems and customer-facing processes. Cybercriminals and malicious state actors are targeting vulnerabilities in remote applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt

Launches," (April 21, 2020); Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Notification, "Defending Against COVID-19 Cyber Scams," (March 6, 2020); Europol Report, "Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis," (March 27, 2020); DHS CISA and Federal Bureau of Investigation (FBI) Public Service Announcement, "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations," (May 13, 2020); FBI's Internet Crime Complaint Center (IC3) Public Service Announcement, "Increased Use of Mobile Banking Apps Could Lead to Exploitation," (June 10, 2020); and DHS CISA, National Security Agency, NCSC, and Canada Communications Security Establishment Joint Advisory, "APT29 Targets COVID-19 Vaccine Development," (July 16, 2020).

[15] For the purpose of this advisory, cyber-enabled crime refers to illegal activities (e.g., fraud, identity theft, etc.) carried out or facilitated by electronic systems and devices, such as networks and computers. *See* FinCEN Advisory, FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," (October 25, 2016).

© gettechnical inc 2021

business operations.[16] Remote identity processes [17] also face significant risks, which may include:

• *Digital Manipulation of Identity Documentation*: Criminals often seek to undermine online identity verification processes through the use of fraudulent identity documents, which can be created by manipulating digital images of legitimate government-issued identity documents to alter the information and/or photos displayed. [18]

• *Leveraging Compromised Credentials Across Accounts*: Cybercriminals commonly undermine weak authentication processes in attempted account takeovers via methods such as credential stuffing attacks. In these attacks, cybercriminals generally use lists of stolen account credentials (typically usernames or email addresses, and associated passwords) to conduct automated login attempts to gain unauthorized access to victim accounts.

Financial red flag indicators of this sort of activity may include:[19]

1. The spelling of names in account information does not match the government-issued identity documentation provided for online onboarding.

---

[16] For information related to publicly disclosed cybersecurity vulnerabilities and exposures, *see* U.S. Department of Commerce, National Institute for Standards and Technology (NIST), "National Vulnerability Database;" MITRE, "Common Vulnerabilities and Exposures: CVE List Home;" and FBI IC3 Public Service Announcements, "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments," (April 1, 2020) and "Increased Use of Mobile Banking Apps Could Lead to Exploitation," (June 10, 2020). *See also* FinCEN Director Kenneth A. Blanco's, prepared remarks delivered at the Consensus Blockchain Conference, "Consensus Blockchain Conference (Virtual)," (May 13, 2020).

[17] For the purposes of this advisory, "remote identity processes" include remote processes for customer onboarding and identity verification, as well as authentication of customers for account access purposes. For more information on digital identity standards, *see* NIST, "Digital Identity Guidelines," (December 1, 2017), and the Financial Action Task Force (FATF), "Guidance on Digital Identity," (March 6, 2020).

[18] Criminals exploiting identity verification processes will typically use either information associated with a real individual's identity (i.e., identity theft) or create a new fabricated identity that usually consists of a real identifier, such as a social security number or driver's license number, with other fake information (i.e., synthetic identity fraud). For more information on example typologies and financial red flag indicators involving identity theft and identity fraud, *see* FinCEN Report, "Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports," (October 2010).

[19] 6. *Id*. *See also* Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, 16 CFR Part 681, app. A.

© gettechnical inc 2021

2. Pictures in identity documentation, especially areas around faces, are blurry or low resolution, or have aberrations. Pictures in identity documentation or other images of persons in remote identity verification [20] show visual signs indicating possible image manipulation (e.g., incongruences in coloration near the edge of the face, or double edges or lines on delineated facial features).
3. Images of identity documentation have visual irregularities that indicate digital manipulation of the images, especially around information fields likely to have been changed to conduct synthetic identity fraud (e.g., name, address, and other identifiers).
4. A customer's physical description on identity documentation does not match other images of the customer.
5. A customer refuse to provide supplemental identity documentation or delays producing supplemental documentation.
6. Customer logins occur from a single device or Internal Protocol (IP) address across multiple seemingly unrelated accounts, often within a short period of time.
7. The IP address associated with logins does not match the stated address in identity documentation.
8. Customer logins occur within a patter of high network traffic with decreased login success rates and increased password reset rates.
9. A customer calls a financial institution to change account communication methods and authentication information, then quickly attempts to conduct transactions to an account that never previously received payments from the customer.

Phishing, Malware, and Extortion

FinCEN and U.S. law enforcement have observed significant increases in broad-based and targeted phishing campaigns that are attempting to lure companies, especially healthcare and pharmaceutical providers, with offers of COVID-19 information and supplies. [21] Phishing scams target individuals with communications appearing to come from legitimate sources to collect victims' personal and financial data and potentially infect their devices by convincing the target to download malicious programs. [22] Cybercriminals usually send these phishing communications by email but may also use phone calls or text messages.

---

[20] Images in identity verification other than identity documentation may include pictures or video of the customer (e.g., "selfie" images) taken as part of the financial institution's onboarding process.

[21] The U.S. Secret Service (USSS) and DHS CISA have noted an increase in malware, phishing, and extortion campaigns related to COVID-19. *See* USSS Press Release, "Secret Service Issues COVID-19 (Coronavirus) Phishing Alert," (March 9, 2020).

[22] *See* DHS CISA and U.K. NCSC Joint Alert (AA20-099A), "COVID-19 Exploited by

© gettechnical inc 2021

In these new schemes, phishing scammers will often reference COVID-19 themes, such as payments related to the Coronavirus Aid, Relief, and Economic Security (CARES) Act, [23] in the subjects and bodies of emails. Some phishing emails lure victims by advertising ways to make money, such as through investing in convertible virtual currencies (CVCs) or via domain names that mimic names of organizations, including those that provide or enable teleworking capabilities.[24] Cybercriminals are also distributing malware, [25] including ransomware, through phishing emails, malicious websites and downloads, domain name system (DNS) hijacking or spoofing attacks, and fraudulent mobile applications. These techniques can be applied in broader campaigns involving social media, such as the recent exploit targeting Twitter and prominent users of the platform. [26] Financial institutions dealing in CVC should be especially alert to the potential use of their institutions to launder proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes and take appropriate risk mitigating steps consistent with their BSA obligations.

FinCEN assesses that instances of extortion will also continue to grow in the wake of the COVID-19 pandemic. So far in 2020, FinCEN has received numerous suspicious activity reports (SARs) involving ransomware [27] targeting medical centers and municipalities. Much of this ransomware was delivered by exploiting the COVID-19 lures described above. We expect criminals to continue targeting entities that are vulnerable due to their involvement

---

Malicious Cyber Actors," (April 8, 2020); and DHS, "Common Scams: Know How to Spot a Fake."

[23] Pub. L. 116–136, 116th Congress (2020).

[24] Since January 2020, tens of thousands of new domains have been registered with terms related to COVID-19 and/or disaster and healthcare response efforts (e.g., "quarantine," "vaccine," and "CDC"), many including or mimicking names of companies that provide or enable teleworking capabilities. U.S. law enforcement agencies have disrupted hundreds of malicious domains used to exploit the pandemic. *See* FinCEN Advisory, FIN-2020-A003, "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020). *See also*, FBI Press Release, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," (April 13, 2020).

[25] Malware can enable criminals to access compromised computers and computer systems to steal credentials, exfiltrate sensitive information through mechanisms like screenshots or keylogging, alter account information, and conduct fraudulent transactions.

[26] *See* FinCEN Alert, FIN-2020-Alert001, "FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter," (July 16, 2020).

[27] Ransomware, a specific type of malware, typically encrypts data on systems in the interest of extorting ransom payment from victims in exchange for decrypting the information and giving victims access to their systems again.

© gettechnical inc 2021

in pandemic response, such as researchers working on medical treatments or manufacturers of personal protective equipment. In other instances of extortion, criminals are threatening to expose victims and their families to COVID-19 if they do not pay the extortion fee. In almost all cases, criminals require ransomware-related extortion payments to be made in CVC. [28]

Financial red flag indicators of this sort of activity may include the following:

10. Information technology enterprise activity related to transaction processes or information is connected to cyber indicators that have been associated with possible illicit activity. Malicious cyber activity may be evident in system log files, network traffic, or file information. [29]
11. Email addresses purportedly related to COVID-19 do not match the name of the sender or the corresponding domain of the company allegedly sending the messages.
12. Unsolicited emails related to COVID-19 from untrusted sources encourage readers to open embedded links/files or to provide personal or financial information, such as usernames and passwords or other account credentials.
13. Emails from untrusted sources or addresses similar to legitimate telework vendor accounts offer remote application software, often advertised at no or reduced cost.
14. Emails contain subject lines identified by government or industry as associated with phishing campaigns (e.g., "Coronavirus Updates," "2019-nCov: new confirmed cases in your City," and "2019-nCoc: Coronavirus outbreak in your City (Emergency)").

[28] Financial institutions dealing in CVC should be especially alert to the laundering of proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes. *See* FinCEN Advisory, FIN-2019-003, "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).

[29] Because cyber indicators are helpful red flag indicators that financial institutions can use to identify related suspicious financial activity, FinCEN, DHS CISA, and the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) offer a broad range of helpful cyber indicator resources, including, but not limited to: FinCEN's Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; OCCIP's CILs and circulars, available upon request; and DHS CISA's cyber analytic products and services, including a comprehensive list of COVID-19-related indicators of compromise in CSV or STIX-formatted XML formats, the Cyber Information Sharing and Collaboration Program (CISCP), and the Automated Indicator Sharing (AIS) program. Public-private and industry partnerships, such as the Financial Services Information Sharing and Analysis Center, and open source and commercial cyber threat feeds can also be useful resources.

© gettechnical inc 2021

15. Text messages have embedded links purporting to be from or associated with government relief programs and payments.
16. Embedded links or webpages addresses for purported COVID-19 resources have irregular uniform resource locators (URLs) that do not match that of the expected destination site or are similar to legitimate sites but with slight variations in the domain (e.g., variations in domain extensions like ".com" ".org" and ".us") or web address spelling.

Business Email Compromise (BEC) Schemes

Cybercriminals have increasingly exploited the COVID-19 pandemic by using BEC schemes, particularly targeting municipalities and the healthcare industry supply chain. A common BEC scheme involves criminals convincing companies to redirect payments to new accounts, while claiming the modification is due to pandemic-related changes in business operations. BEC criminals often use spoofed or compromised email accounts to communicate these urgent, last-minute payment changes. In the COVID-19 environment, criminals insert themselves into communications by impersonating a critical player in a business relationship or transaction, typically posing as providers of healthcare supplies, to intercept or fraudulently induce a payment for critically needed supplies. [30]

Financial red flag indicators of this sort of activity may include the following: [31]

17. A customer's transaction instructions contain different language, timing, and amounts in comparison to prior transaction instructions, especially regarding transactions involving healthcare providers or supplies purchases.
18. Transaction instructions, typically involving a healthcare-sector counterparty or referencing purchase of healthcare or emergency response supplies, originate from an email account closely resembling, but not identical to, a known customer's email account.

---

[30] *See* FBI Press Release, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," (April 6, 2020). *See also* Europol Press Release, "Corona Crimes: Suspect Behind €6 Million Face Masks and Hand Sanitisers Scam Arrested Thanks to International Police Cooperation," (April 6, 2020).

[31] For general BEC-scheme financial red flag indicators, *see* FinCEN Advisories, FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes," (September 6, 2016), and FIN-2019-A005, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019).

© gettechnical inc 2021

19. Emailed transaction instructions direct payment to a different account for a known beneficiary. The transmitter may claim a need to change the destination account as part of a COVID-19 pandemic response, such as moving the account to a financial institution in a jurisdiction less affected by the disease, and assert urgency to conduct the transaction.
20. Emailed transaction instructions request to move payment methods from checks to ACH transfers as a response to the pandemic.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN and law enforcement's ability to effectively identify and pull actionable SARs and information from the FinCEN Query system to support COVID-19-related cases.

• FinCEN requests that financial institutions reference this advisory by including the key term "**COVID19-CYBER FIN-2020-A005**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

• Financial institutions that suspect fraudulent COVID-19-related activity should mark all appropriate check boxes on the SAR form to indicate a connection between COVID-19 and the suspicious activity being reported. For example, if the activity includes a COVID-19-related account takeover involving an ACH transfer, financial institutions can select SAR field 38a and 38z, and note in the "other" box, "COVID-19 account takeover fraud – ACH."[32]

• Financial institutions should also include any relevant technical cyber indicators related to cyber events and associated transactions reported in a SAR within the available structured cyber event indicator fields. For example, for a COVID-19-related cyber event against a financial institution, financial institutions can select SAR field s 42a and 42z

[32] 19. For additional guidance on identifying account takeover activity and related SAR filing instructions, *see* FinCEN Advisory, FIN-2011-A016, "Account Takeover Activity," (December 19, 2011).

© gettechnical inc 2021

(noting in the "other" box the COVID-19-related cyber event), and SAR fields 44(a)-(j), (z), including email or CVC wallet addresses, malicious domains or URLs, and any other known cyber event indicators.

• For cyber-enabled crime involving fraud driven by COVID-19, financial institutions should select SAR field 34z (Fraud – other) as the associated suspicious activity type. Additionally, financial institutions should include the type of cybercrime or scheme as a keyword (e.g., "COVID 19 BEC Fraud," "EAC fraud," or "BEC data theft") in SAR field 34(z).

• Please refer to FinCEN's May 18, 2020 Notice Related to the Coronavirus Disease 2019, which contains information regarding reporting COVID-19-related crime and FinCEN's Rapid Response Program, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

© gettechnical inc 2021

FinCEN ADVISORY

FIN-2020-A003 July 7, 2020

Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)

Detecting, preventing, and reporting consumer fraud and other illicit activity related to COVID-19 is critical to our national security, safeguarding legitimate relief efforts, and protecting innocent people from harm.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of imposter scams and money mule schemes, which are two forms of consumer fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of imposter scams and money mule schemes, financial red flag indicators for both, and information on reporting suspicious activity. This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will issue COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at https://www.fincen.gov/coronavirus, which also contains information on registering to receive FinCEN Updates.

Financial Red Flag Indicators of COVID-19 Imposter Scams and Money Mule Schemes

Consumer frauds include imposter scams and money mule schemes, where actors deceive victims by impersonating federal government agencies, international organizations, or charities. FinCEN identified the financial red flag indicators described below to alert financial institutions to these frauds and to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic.

© gettechnical inc 2021

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities.

Imposter Scams

In imposter scams, criminals impersonate organizations such as government agencies, non-profit groups, universities, or charities to offer fraudulent services or otherwise defraud victims. While imposter scams can take multiple forms, the basic methodology involves an actor (1) contacting a target under the false pretense of representing an official organization, and (2) coercing or convincing the target to provide funds or valuable information, engage in behavior that causes the target's computer to be infected with malware, or spread disinformation. [33] In the case of schemes connected to COVID-19, imposters may pose as officials or representatives from the Internal Revenue Service (IRS), [34] the Centers for Disease Control and Prevention (CDC),[35] the World Health Organization (WHO), other healthcare or non-profit groups, and academic institutions.[36] Illicit actors can use imposter scams to defraud and deceive the vulnerable, including the elderly and unemployed, through the solicitation of payments (such as digital payments and virtual currency), donations, or personal information via email, robocalls, text messages,[37] or other communication methods. For example, an imposter may contact potential victims by phone, email, or text to imply that the victim must verify personal information or send payments to scammers in return for COVID-19-related stimulus payments or benefits, including Economic Impact Payments (EIP)[38] under the Coronavirus Aid, Relief, and Economic Security

[33] *See* Federal Trade Commission (FTC) Business Blog, "Seven Coronavirus Scams Targeting Your Business," (March 25, 2020).
[34] For information on IRS imposter scams in general, *see* FTC's "IRS Imposter Scams Infographic," (January 2020).
[35] *3.See* Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) Public Service Announcement "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic," (March 20, 2020).
[36] FTC maintains links to resources concerning scams and the current trends it has observed. *See* FTC's "Coronavirus Advice for Consumers."
[37] For information about COVID-19-related imposter scams conducted by text messages and phone calls, see the Federal Communications Commission (FCC), "COVID-19 Consumer Warnings and Safety Tips," (May 20, 2020). The FTC and the FCC have sent warning letters to multiple Voice over Internet Protocol (VoIP) service providers for allegedly routing illegal pandemic-related scam telemarketing or robocalls. *See* FTC Press Release, "FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls," (May 20, 2020).
[38] EIP may take the form of Automated Clearing House (ACH) deposits, U.S. Treasury checks,

© gettechnical inc 2021

(CARES) Act.[39] Another instance includes imposters contacting victims and posing as government or health care representatives engaged in COVID-19 contact tracing activities, implying that a victim must share personal or financial information as part of contact tracing efforts.[40] Multiple examples include phishing schemes, where imposters send communications appearing to come from legitimate sources, to collect victims' personal and financial data and potentially infect their devices by convincing the target to download a malicious attachment or click malicious links.[41]
Scammers may also impersonate legitimate charities or create sham charities, taking advantage of the generosity of the public and embezzling donations intended for COVID-19 response efforts.[42]

Criminals often use social media accounts, door-to-door collections, flyers, mailings, telephone and robocalls, text messages, websites, and emails mimicking legitimate charities and non-profits to defraud the public. These operations may include words like "relief," "fund," "donation," and "foundation" in their titles to give the illusion that they are a legitimate organization.[43]

---

or prepaid debit cards. *See* U.S. Department of the Treasury (Treasury) Press Release "Treasury is Delivering Millions of Economic Impact Payments by Prepaid Debit Card," (May 18, 2020).

[39] The FTC, the IRS, and the Treasury Inspector General for Tax Administration (TIGTA) each published information about imposter scams, particularly as they relate to EIP. *See* FTC Blog, "Want to Get Your Coronavirus Relief Check? Scammers do too," (April 1, 2020) and "Coronavirus Checks: Flattening the Scam Curve," (April 8, 2020); IRS News Release, "IRS Issues Warning About Coronavirus-related Scams; Watch Out For Schemes Tied To Economic Impact Payments," (April 2, 2020) and the IRS's Economic Impact Payment Information Center, (April 8, 2020); and TIGTA Press Release, "TIGTA Urges Taxpayers to "Be On High Alert" For Coronavirus Relief Payment Scams," (April 7, 2020).

[40] *See* Department of Justice (DOJ) Press Release "U.S. Attorney Warns Public of COVID-19 Contact Tracing Frauds," (May 28, 2020).

[41] *See* Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's (U.K.) National Cyber Security Centre (NCSC) Alert, "COVID-19 Exploited by Malicious Cyber Actors" (April 8, 2020); and DHS, "Common Scams: Know How to Spot a Fake." Additionally, *see* WHO Cybersecurity, "Beware of Criminals Pretending to be WHO," (April 2020). *See also* FTC Blog, "COVID-19 Scams Targeting College Students," (May 27, 2020); and DOJ Press Release, "Federal Law Enforcement Encourages the Public to Remain Vigilant to Covid-19 Scams," (April 22, 2020).

[42] 10. Multiple U.S. Attorneys' Offices (USAOs) warn of criminals who may seek to exploit legitimate relief efforts for their own illicit gain by soliciting donations to sham charities or crowdfunding sites. *See* USAO for the Southern District of Georgia, "U.S. Attorney Warns of Coronavirus Scams Targeting Vulnerable Victims," (March 25, 2020); USAO for the Eastern District of Oklahoma, "Department of Justice Requests Citizens be Aware of And Report COVID-19 Fraud," (March 24, 2020); and USAO for the Middle District of Tennessee, "U.S. Attorney and FBI Urge the Public to Report Suspected Fraud Related to Tornado Destruction and COVID-19," (March 23, 2020). Additionally, the U.S. Securities and Exchange Commission (SEC) noted the potential for charity investment frauds, where actors falsely claim that investments will provide financial support or medical treatment to people in need, with the money instead stolen. *See* SEC Investor Alerts and Bulletins, "Frauds Targeting Main Street Investors -- Investor Alert," (April 10, 2020). *See also* FTC's information to avoid charity scams, "Make Your Coronavirus Donations Count," (May 5, 2020).

[43] *See* FTC, "How to Donate Wisely and Avoid Charity Scams."

© gettechnical inc 2021

Given that many scammers may be targeting customers as opposed to financial institutions directly, financial institutions, when interacting with their customers, should remain on the alert for potential suspicious activities. Financial red flag indicators of imposter scams may include:

1. A customer indicating that a person claiming to represent a government agency contacted him or her by phone, email, text message, or social media asking for personal or bank account information to verify, process, or expedite EIPs, unemployment insurance, or other benefits. [44] In particular, be alert to communications emphasizing "stimulus check" or "stimulus payment" in solicitations to the public, sometimes claiming that the fraudulent entity can expedite the "stimulus check" or other government payment on behalf of the beneficiary for a fee paid by gift card or prepaid card.
2. Receipt of document that appears to be a check or a prepaid debit card from the U.S. Treasury, often in an amount less than the expected EIP, with instructions to contact the fraudulent government agency, via a phone number or online, to verify personal information in order to receive the entire benefit.
3. Unsolicited communications from purported trusted sources or government programs related to COVID-19, instructing reader to open embedded links or files or to provide personal or financial information, including account credentials (e.g., usernames and passwords).
4. Email addresses in COVID-19 correspondence that do not match the name of the sender, contain misspellings, or do not end in the corresponding domain of the organization from which the message allegedly was sent. For example, government agencies will use ".gov" or ".mil." Many legitimate charities will use ".org" WHO emails will contain "@who.int." Fraudsters, however, may use ".com" or ".biz" in place of the expected domain.
5. Email correspondence that contains subject lines that government or industry have identified as being associated with phishing campaigns, or that contains embedded links or webpage addresses for purported COVID-19 resources that have irregular URLs (e.g., slight variations in domain extensions like ".com," ".org," and ".us"). Examples of U.S. government-identified COVID-19 phishing email subject lines include "2020 Coronavirus Updates," "Coronavirus Updates," "2019-nCov: New confirmed cases in your City," and "2019-nCov: Coronavirus outbreak in your city (Emergency)." [45]
6. Solicitations where the person, email, or social media advertisement seeks donations on behalf of a reputable organization, but is not affiliated with the

[44] For more information on EIPs, visit IRS, "Economic Impact Payment Information Center," (June 30, 2020).

[45] *See* DHS CISA and U.K. NCSC Alert, "COVID-19 Exploited by Malicious Cyber Actors," (April 8, 2020).

© gettechnical inc 2021

reputable organization (e.g., the solicitor is not recognized or endorsed as an employee or volunteer by the organization, the email address is misspelled or not connected to the organization, or the social media advertisement directs individuals to an unaffiliated website).

7. A charitable organization soliciting donations that (1) does not have an in-depth history, financial reports, IRS annual returns, documentation of their tax-exempt status, or (2) cannot be verified by using various internet-based resources that may assist in confirming the group's existence and its nonprofit status.

Money Mule Schemes

A money mule is "a person who transfers illegally acquired money on behalf of or at the direction of another."[46] Money mule schemes, including those related to the COVID-19 pandemic, span the spectrum of using unwitting, witting, or complicit money mules.[47] An **unwitting** or **unknowing** money mule is an individual who is "unaware that he or she is part of a larger criminal scheme." The individual is motivated by his/her trust in the actual romance, job position or proposition.[48] A **witting** money mule is an individual who "chooses to ignore obvious red flags or acts willfully blind to his/ her money movement activity." The individual is motivated by financial gain or an unwillingness to acknowledge his/her role.[49] A **complicit** money mule is an individual who is "aware of his/her role as a money mule and is complicit in the larger criminal scheme." The individual is motivated by financial gain or loyalty to a criminal group.[50] During the COVID-19 pandemic, U.S. authorities have detected recruiters using money mule schemes, such as good-Samaritan, romance, and work-from-home schemes.[51] U.S. authorities also have identified criminals

---

[46] *See* FBI, "Money Mule Awareness" (July 2019). For more information on money mules in general, *see* FinCEN, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019); "FinCEN Analysis: Bank Secrecy Act Reports Filed by Financial Institutions Help Protect Elders from Fraud and Theft of Their Assets," (December 4, 2019); and DOJ, "Justice Department Announces Landmark Money Mule Initiative," (December 4, 2019).

[47] For more information about unwitting, witting, and complicit individuals involved in money mule scams, *see* FBI, "Money Mule Awareness" (July 2019).

[48] For examples of how an unwitting money mule is recruited and used, *see id*., p. 4.

[49] For examples of how a witting money mule is recruited and used, *see id*., p. 5.

[50] For examples of how a complicit money mule is recruited and used, *see id*.

[51] The FBI has released information on how criminals are taking advantage of the COVID-19 pandemic to steal money, access personal and financial information, and use individuals as money mules. *See* FBI Press Release, "FBI Warns of Money Mule Schemes Exploiting the COVID-19 Pandemic," (April 6, 2020). In work-from-home schemes, for example, COVID-19 money mule recruiters, under a false charity or company label,

© gettechnical inc 2021

using money mules to exploit unemployment insurance programs during the COVID-19 pandemic.[52] Financial red flag indicators of COVID-19 money mule schemes may include:

8. The customer's personal bank account starts to receive transactions that do not fit his or her transactional history profile, including overseas transactions, the purchase of large sums of convertible virtual currency, or transactions in large fiat amounts, or the account generally had a low balance until the customer became involved in a money mule scheme. When asked about the changes in transactions, the customer declines requests for "know your customer" documents or inquires regarding sources of funds, and may mention COVID-19, relief work, or a "work-from-home" opportunity as the source of the income.
9. The customer opens a new bank account in the name of a business and, shortly thereafter, someone transfers the funds out of the account. The person transferring the funds could be the registered accountholder or someone else, and may keep a portion of the money he or she transferred (per instruction of the scammer). While this activity, in and of itself, may not be suspicious, it may become so if the individual provides unsatisfactory answers to the financial institution's inquiries, declines to provide essential "know your customer" documents, or mentions COVID-19, relief work, or a "work-from-home" opportunities as the source of the funds.
10. The customer opens accounts in his or her name at multiple banks so he or she may receive money from various individuals or businesses, then moves the money to other accounts at the direction of the customer's purported employer.
11. The customer receives multiple state unemployment insurance payments to his or her account, or to multiple accounts held at the same financial institution, within the same disbursement timeframe (e.g., weekly or biweekly payments) issued from one or multiple states.

---

may approach targets with a seemingly legitimate offer of employment under the pretense of work-from-home jobs, often through internet or social media advertisements, emails, or text messages. Once the target accepts the "employment," he or she receives instructions to move funds through accounts or to set up a new account in the target's name for the "business." The target (i.e., the money mule) earns money by taking a percentage of the funds that he or she helps to transfer per the instructions of the "employer." For more information on fraudulent job offers, *see* FTC Blog, "Looking for work after Coronavirus layoffs?," (April 13, 2020).

[52] *See* Washington State Employment Security Department, "Statement from Commissioner Suzi LeVine on the rise in unemployment imposter fraud attempts," (May 14, 2020) and "Update on imposter fraud from Commissioner Suzi LeVine," (May 18, 2020).

© gettechnical inc 2021

12. The customer's account(s) receives an unemployment deposit from a different state in which he or she reportedly resides or has previously worked.
13. The customer's account receives unemployment insurance payments for numerous employees or the accountholder name and ACH payment "remit to" name do not match.
14. Deposited funds are quickly diverted via wire transaction to foreign accounts located within countries known for having poor anti-money laundering controls.
15. The customer makes one or more atypical transactions involving an overseas account, especially through unusual payment methods for the customer. When asked about the transaction, the customer indicates it is for a person located overseas who is in need of financial assistance because of COVID-19 pandemic.
16. Documentation from the customer shows that the purported employer or recruiter uses a common web-based, free email service instead of a company-specific email. For example, instead of a company-or organization-specific email address, such as first.lastname@ABCcompany.com or lastname@XYZ_NGO.org , the email address is from a common and free email address provider.
17. The customer provides information that his or her purported employer asked the customer to receive funds into his or her personal bank account, so that the employer can then process or transfer funds via wire transfer, ACH, mail, or money services businesses out of the customer's personal account.
18. The customer states, or information shows, that an individual, whom the customer may not have known previously, requested financial assistance to send/receive funds through the customer's personal account, including requests by individuals claiming to be a:
    a. U.S. Service member who is reportedly stational abroad;
    b. U.S. Citizen working or traveling abroad; or
    c. U.S. Citizen quarantined abroad.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN's and law enforcement's abilities to effectively identify actionable SARs using the FinCEN Query system and pull information to support COVID-19- related investigations.

- FinCEN requests that financial institutions reference this advisory by including the key term "COVID19 MM FIN-2020-A003" in SAR field 2 (Filing Institution Note to FinCEN) and

the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

- Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., imposter scam or money mule scheme) in SAR field 34(z). In addition, FinCEN encourages financial institutions to report certain types of imposter scams and money mule schemes using fields such as SAR fi eld 34(l) (Fraud-Mass-marketing), or SAR field 38(d) (Other Suspicious Activities- Elder Financial Exploitation), as appropriate with the circumstances of the suspected activity.
- Please refer to FinCEN's **Notice Related to the Coronavirus Disease 2019** (COVID-19), which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

FinCEN NOTICE

May 18, 2020

Notice Related to the Coronavirus Disease 2019 (COVID-19)

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice as part of FinCEN's COVID-19-related response. This Notice contains pertinent information regarding reporting COVID-19-related criminal and suspicious activity and reminds financial institutions of certain Bank Secrecy Act (BSA) obligations. FinCEN intends to issue multiple COVID-19-related advisories. Each advisory will refer financial institutions to this Notice.

COVID-19-Related Updates to Financial Institutions

FinCEN has published notices on its website that provide information to assist financial institutions in complying with their BSA obligations during the COVID-19 pandemic, which include a direct contact mechanism for urgent COVID-19-related issues. FinCEN encourages financial institutions to monitor FinCEN's website and the Department of the Treasury's website on The Coronavirus Aid, Relief, and Economic Security (CARES) Act for up-to-date information concerning compliance with BSA obligations. [53]

BSA Reporting Obligations

Compliance with the BSA remains crucial to protecting our national security by combating money laundering and related crimes, including terrorism and its financing. FinCEN expects financial institutions to continue following a risk-based approach and to diligently adhere to their BSA obligations. FinCEN also appreciates that financial institutions are taking actions to protect employees, their families, and others in response to the COVID-19 pandemic. FinCEN recognizes that current circumstances may create challenges with respect to certain BSA obligations, including the timing requirements for certain BSA report filings. FinCEN will continue outreach to regulatory partners and financial institutions to

[53] For up-to-date information on FinCEN's COVID-19-related releases, please visit FinCEN's Coronavirus Updates at https://www.fincen.gov/coronavirus. Those interested in receiving notifications from FinCEN may sign up for FinCEN Updates, at no charge, to receive updates with links to new information when content is added to FinCEN's website for any of the enrolled user's selected categories. For up-to-date information concerning the Department of the Treasury's CARES Act information, please visit https://home.treasury.gov/policy-issues/cares.

© gettechnical inc 2021

ensure risk-based compliance with the BSA, and FinCEN will issue additional information as appropriate. [54]

Financial institutions that wish to communicate their organizational COVID-19-related concerns, such as issues with the timely filing of BSA reports, should go to www.fincen.gov, click on "Need Assistance," and select "COVID19" in the subject drop-down list.

SAR Filing Instructions

In light of the COVID-19 pandemic, some financial institutions have added COVID-19 statements to their disclaimers or are using SAR narratives to address COVID-19's impact on their SAR filing abilities. Financial institutions should not include in the SAR narrative their challenges during the pandemic; the SAR narrative should include COVID-19 when it is tied to suspicious activity only. However, filers who have already included references to COVID-19 in matters not related to the pandemic do not need to file corrected reports.

Provision of SAR Supporting Documentation to Law Enforcement and FinCEN

In order to effectively respond to and combat fraud schemes, (e.g. those exploiting the COVID-19 pandemic), law enforcement and FinCEN require full details related to SAR filings, including supporting documentation, as quickly as possible.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. [55] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. [56] When requested to provide supporting documentation, financial institutions should verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. Disclosure of SARs and supporting documentation to appropriate law enforcement and supervisory agencies is protected by the safe harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions. [57]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving fraud schemes, including those related to COVID-19. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions

---

[54] *See* FinCEN Notice, "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic," (April 3, 2020).

[55] *See* 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).

[56] *Id. See also* FinCEN Guidance, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

[57] *See* 31 U.S.C. § 5318(g)(3).

© gettechnical inc 2021

that the institution suspects may involve the proceeds of one or more specified unlawful activities ("SUAs") and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including fraud against individuals or the government. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs. [58]

Reporting COVID-19-Related Criminal Activity

There are a variety of U.S. government agencies positioned to assist in investigating and combating COVID-19-related criminal activity. Financial institutions and their customers should consider reporting COVID-19 crimes to the following agencies: *COVID-19-Related Fraud Schemes:* Department of Justice (DOJ) urges the public to report suspected fraud schemes related to COVID-19 by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721).[59] The NCDF can receive and enter complaints into a centralized system that can be accessed by all U.S. Attorney Offices, as well as DOJ law enforcement components, to identify, investigate, and prosecute fraud schemes. The NCDF coordinates complaints with 16 additional federal law enforcement agencies, as well as state Attorneys General and local authorities. The public may also report CARES Act-related fraud or other COVID-19-related financial crime to the U.S. Secret Ser vice (USSS) by contacting their local USSS field office. Additionally, Department of Homeland Security (DHS) (including Homeland Security Investigations (HSI) and Immigration and Customs Enforcement) encourages the reporting of COVID-19 financial, cyber, and import/export fraud via the Operation Stolen Promise website / intake email address.

Cyber- and Internet-related Crime: Federal Bureau of Investigation's (FBI) Crime Complaint Center (IC3);[60]

the DHS's CISA National Cybersecurity Communications and Integration Center (NCCIC); and HSI's Operation Stolen Promise fraud intake.[61]

---

[58] For further guidance related to the 314(b) Program, see FinCEN Fact Sheet, "Section 314(b)" (November 2016) and FinCEN Guidance, FIN-2009-G002, "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," (June 16, 2009).

[59] *See* DOJ Press Release, "Attorney General William P. Barr Urges American Public to Report COVID-19 Fraud," (March 20, 2020).

[60] *See* the FBI's IC3 website, https://www.ic3.gov/.

[61] *See* HSI "Operation Stolen Promise" website, HSI COVID-19 Fraud website, https://www.ice.gov/topics/operation-stolen-promise.

© gettechnical inc 2021

Identity Theft and Fraud: The Federal Trade Commission and the Social Security Administration fraud hotline (1-800-269-0271).
Federal Tax Fraud: Fraud involving payment of federal taxes should be reported t o the Treasury Inspector General for Tax Administration.

Response and Recovery of Funds

To better assist the public during the COVID-19 pandemic, FinCEN has temporarily expanded its Rapid Response Program to support law enforcement and financial institutions in the recovery of funds stolen via fraud, theft, and other financial crimes related to COVID-19. FinCEN has already been involved in multiple Rapid Response matters involving allegations of COVID-19 fraud, to include assisting in the recovery of $300 million in one case. To request immediate assistance in recovering cybercrime- and COVID-19-related stolen funds, financial institutions should file a complaint with the FBI's IC3, contact their local FBI field office, or contact the nearest USSS field office. Contacting law enforcement for fund recovery assistance does not relieve a financial institution from its SAR filing obligations. FinCEN, in partnership with the FBI, the USSS, HSI, and the U.S. Postal Inspection Service, as well as counterpart Financial Intelligence Units abroad, can help financial institutions recover funds stolen as the result of business email compromise (BEC) and cybercrime schemes through its Rapid Response Program. Through these partnerships, FinCEN has successfully assisted in the recovery of approximately $900 million with the assistance of 64 countries. While FinCEN does not ensure recovery of BEC stolen funds, FinCEN has achieved greater success in recovering funds when victims or financial institutions report BEC-unauthorized and fraudulently induced wire transfers to law enforcement within 24 hours.

© gettechnical inc 2021

FinCEN ADVISORY

FIN-2020-A002 May 18, 2020

Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to rising medical scams related to the COVID-19 pandemic. This advisory contains descriptions of COVID-19-related medical scams, case studies, red flags, and information on reporting suspicious activity.[62]

This is the first of several advisories FinCEN intends to issue concerning financial crimes related to the COVID-19 pandemic. These advisories are based on FinCEN's analysis of COVID-19-related information obtained through public reports, Bank Secrecy Act (BSA) data, and law enforcement partners. FinCEN will issue financial analyses and intelligence, as appropriate, to financial institutions to help them detect, prevent, and report suspected illicit activity.[63] Additionally, FinCEN has temporarily expanded its Rapid Response Program, which supports law enforcement and financial institutions in the recovery of funds stolen via fraud, theft, and other financial crimes related to COVID-19.

Financial Red Flag Indicators of COVID-19 Fraudulent Activity

BSA data, as well as information from other federal agencies, foreign government partners, and public sources indicate possible illicit activities related to the COVID-19 pandemic regarding (1) fraudulent cures, tests, vaccines, and services; (2) non-delivery scams; and (3) price gouging and hoarding of medical-related items, such as face masks and hand sanitizer. FinCEN identified the following red flag indicators to help financial institutions identify COVID-19-related medical scams, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic.

[62] While this advisory focuses on medical-related scams, financial institutions should note that criminal actors may use similar fraudulent methods involving non-medical-related goods or services. Many COVID-19-related scams are similar to those observed before the pandemic, and illicit actors have modified their schemes to take advantage of, and profit from, the pandemic by victimizing innocent people and businesses.

[63] For up-to-date information on FinCEN COVID-19-related releases, please visit FinCEN Coronavirus Updates at https://www.fincen.gov/coronavirus.

© gettechnical inc 2021

As no single red flag is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple indicators, before determining if a transaction is suspicious or otherwise indicative of fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate. Some of these red flags are common indicators of fraudulent merchant activity committed by shell or fraudulent retail or wholesale business operators. Additionally, some of the red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities.

Medical-Related Frauds, Including Fraudulent Cures, Tests, Vaccines, and Services

Several federal agencies have detected fraudulent COVID-19-related cures, tests, vaccines, and associated services being offered to the public.[64] Examples of fraudulent medical services include claims related to purported vaccines or cures for COVID-19, claims related to products that purportedly disinfect homes or buildings, and the distribution of fraudulent or unauthorized at-home COVID-19 tests. Some of these scams may be perpetrated by illicit actors who recently formed unregistered or unlicensed medical supply companies. Financial indicators of these scams may include:

1. U.S. authorities, such as the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), or the DOJ, have identified the company, merchant, or business owners as selling fraudulent products. [65]
2. A web-based search or review of advertisements indicates that a merchant is selling at-home COVID-19 tests,[66] vaccines, treatments, or cures.

---

[64] *See* Department of Justice (DOJ) Press Release, "Georgia resident arrested for selling illegal products claiming to protect against viruses," (April 9, 2020); U.S. Department of Homeland Security News Release, "ICE HSI arrests Georgia resident for selling illegal pesticide, claiming it protects against coronavirus," (April 14, 2020); U.S. Customs and Border Protection (CBP) National Media Release, "CBP Officers Seize Fake COVID-19 Test Kits at LAX," (March 14, 2020); FTC Press Release, "FTC, FDA Send Warning Letters to Seven Companies about Unsupported Claims that Products Can Treat or Prevent Coronavirus," (March 9, 2020); and Federal Bureau of Investigation (FBI) Press Releases, "FBI Warns of Emerging Health Care Fraud Schemes Related to COVID-19 Pandemic," (April 13, 2020); and "FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment," (March 27, 2020).

[65] For current lists of COVID-19-related warning letters and fraudulent products, visit FDA: "Fraudulent Coronavirus Disease 2019 (COVID-19) Products" and FTC: "FTC Coronavirus Warning Letters to Companies." For information pertaining to COVID-19-related DOJ actions, visit: "Coronavirus Fraud News."

[66] At the time of this publication, the FDA has authorized three at-home tests: the "LabCorp COVID-19 RT-PCR," the Rutgers Clinical Genomics Laboratory's molecular Laboratory Developed Test, and the Everlywell COVID-19 Test Home Collection Kit. *See* FDA News Release, "Coronavirus (COVID-19) Update: FDA Authorizes First Test for Patient At-Home Sample Collection," (April 21, 2020); FDA News Release, "Coronavirus (COVID-19) Update: FDA

3. The customer engages in transactions to or through personal accounts related to the sale of medical supplies, which could indicate that the selling merchant is an unregistered or unlicensed business or is conducting fraudulent medical-related transactions.

4. The financial institution's customer has a website with one or more indicia of suspicion, including a name/web address similar to real and well-known companies, a limited internet presence, a location outside of the United States, and/or the ability to purchase pharmaceuticals without a prescription when one is usually required.

5. The product's branding images found in an online marketplace appear to be slightly different from the legitimate product's images, which may indicate a counterfeit product.

6. The merchant is advertising the sale of highly sought-after goods related to the COVID-19 pandemic and response at either deeply discounted or highly inflated prices.

7. The merchant is requesting payments that are unusual for the type of transaction or unusual for the industry's pattern of behavior. For example, instead of a credit card payment , the merchant requires a pre-paid card, the use of a money services business, convertible virtual currency, or that the buyer send funds via an electronic funds transfer to a high-risk jurisdiction.

8. Financial institutions might detect patterns of high chargebacks and return rates in their customer's accounts. These patterns can be indicative of merchant fraud in general.

Case Study: U.S. Authorities Take Action Against Fraudulent COVID-19 Tests and Treatments

Non-Delivery Fraud of Medical-Related Goods Scams

The COVID-19 pandemic has disrupted global shipping and created sudden and substantial demand for certain goods, especially medical-related goods. This demand creates a situation where criminals may defraud consumers and companies through non-delivery of merchandise. In these non-delivery scams, a customer pays a company for goods the customer will never receive. These bogus companies advertise test kits, masks,

Authorizes First Diagnostic Test Using At-Home Collection of Saliva Specimens," (May 8, 2020); and FDA News Release, "FDA Authorizes First Standalone At-Home Sample Collection Kit that can be used with Certain Authorized Tests," (May 16, 2020).

© gettechnical inc 2021

drugs, and other goods they never intend to deliver, and sometimes never possess at all. Victims can include unsuspecting companies, hospitals, governments, and consumers. These fraudulent transactions occur through websites, robocalls, or on the Darknet. Some schemes involve shell companies[67] to facilitate transactions. In its March 27, 2020 warning to the health care industry, the FBI asked the medical community to exercise due diligence and appropriate caution when dealing with unfamiliar vendors and when relying on unidentified third-party brokers in the supply chain.[68] Financial indicators of these scams may include:

9. The merchant does not appear to have a lengthy corporate history (e.g., the business was established within the last few months), lacks physical presence or address, or lacks an Employer Identification Number. Additionally, if the merchant has an address, there are noticeable discrepancies between the address and a public record search for the company or the street address, multiple businesses at the same address, or the merchant is located in a high-risk jurisdiction or a region that is not usually associated with the merchandise they are selling.

10. Searches in corporate databases reveal that the merchant's listing contains a vague or inappropriate company name, multiple unrelated names, a suspicious number of name variations, multiple "doing business as" (DBA) names, or does not align with its business model.

11. Merchants are reluctant to provide the customer or the financial institution that is processing the transactions with invoices or other documentation supporting the stated purpose of trade-related payments.

12. The financial institution does not understand the merchant's business model, and has difficulty determining the true nature of the company and its operations.

13. The merchant cannot provide shipment-tracking numbers to the customer or proof of shipment to a financial institution so it may process related financial transactions.

14. The merchant claims several last minute and suspicious delays in shipment or receipt of goods. For example, the merchant claims that the equipment was seized at port or by authorities, that customs has not released the shipment, or that the

[67] Shell companies are defined as non-publicly traded corporations or limited liability companies (LLCs) that have no physical presence beyond a mailing address and generate little to no independent economic value. *See* FinCEN Guidance, FIN-2006-G014 "Potential Money Laundering Risks Related to Shell Companies," (November 2006); and Suspicious Activity Reports (SAR) Activity Review: Issue 1 (October 2000), Issue 2 (June 2001), and Issue 7 (August 2004).

[68] *See* FBI Press Release, "FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment," (March 27, 2020).

shipment is delayed on a vessel and cannot provide any additional information about the vessel to the customer or their financial institution.

15. The merchant cannot explain the source of the goods or how the merchant acquired bulk supplies of highly sought-after goods related to the COVID-19 pandemic.

16. Domestic or foreign governments have identified the merchant or its owners/incorporators as being associated with fraudulent and criminal activities.

17. A newly-opened account receives a large wire transaction that the accountholder failed to mention during the account opening process.

Case Study: A Virginia Financial Institution Alerted the U.S. Secret Service (USSS) and Successfully Helped Prevent a $317 Million Non-Delivery Scam

Price Gouging and Hoarding of Medical-Related Items

FinCEN and DOJ have received numerous reports of suspected hoarding and price gouging related to the COVID-19 pandemic. DOJ established the Hoarding and Price Gouging Task Force on March 24, 2020, to address COVID-19-related market manipulation, hoarding, and price gouging. According to DOJ, hoarding and price gouging are defined as the act by any person or company of accumulating an unreasonable amount of any of these materials for their personal use, or accumulating any of these materials for purposes of selling them far above prevailing market prices.[69] In many cases, individuals have been selling surplus items or newly acquired bulk shipments of goods, such as masks, disposable gloves, isopropyl alcohol, disinfectants, hand sanitizers, toilet paper, and other paper products at inflated prices because of the COVID-19 pandemic. Payment methods vary by scheme and can include the use of pre-paid cards, money services businesses, credit card transactions, wire transactions, or electronic fund transfers. On March 23, 2020, President Trump issued Executive Order (E.O.) 13910, pursuant to section 102 of the Defense Production Act, which prohibits hoarding of designated items.[70] Financial indicators of these scams may include:

---

[69] *See* DOJ, "Department of Justice COVID-19 Hoarding and Price Gouging Task Force," (March 24, 2020).

[70] *See* E.O. 13910, "Executive Order on Preventing Hoarding of Health and Medical Resources to Respond to the Spread of COVID-19," (March 23, 2020). The E.O. does not define hoarding. The E.O delegates the authority to prevent hoarding to the Secretary of Health and Human Services and to designate materials "the supply of which would be threatened by persons accumulating the material either in excess of reasonable demands of business, personal, or home consumption, or for the purpose of resale at prices in excess of prevailing market prices." Furthermore, the Attorney General of the United States stated that the "Department will investigate and prosecute those who acquire vital medical supplies in excess of what they would reasonably use or for the purpose of charging exorbitant prices to the healthcare workers and hospitals who need them." *See* DOJ, "Department of Justice COVID-19 Hoarding and Price Gouging Task Force," (March 24, 2020).

18. In addition to the use of personal accounts for business purposes (*see* indicator number 3 above), a customer begins using their personal accounts for business-related transaction after January 2020, and sets up a medical supply company or is selling highly sought-after COVID-19-related goods online, such as hand sanitizer, toilet paper, masks, and anti-viral or disinfectant cleaning supplies.

19. The customer begins using their money services or bank account differently. For example, prior to January 2020, the customer never linked their account to the sale of goods on the internet. Since the COVID-19 pandemic began, however, the customer is receiving deposits with payment messages indicating that they are for the sale of medical goods, disinfectants, sanitizers, and paper products sold on the internet.

20. The customer's accounts are receiving or sending electronic fund transfers (EFT) to /from a newly established company that has no known physical or internet purpose.

21. The customer's account is used in transactions for COVID-19-related goods, such as masks and gloves, with a company that is not a medical supply distributor, is involved in other non-medical-related industries, or is not known to have repurposed its manufacturing to create medical-related goods. For example, the company is currently selling medical and sanitary supplies, and prior to January 2020, the company was listed as an automotive shop, a lumberyard, or a restaurant.

22. The customer makes unusually large deposits that are inconsistent with the customer's profile or account history. Upon further investigation, the customer states, or open-source research indicates, that the customer was selling COVID-19-related goods not usually sold by the customer.

Case Study: FBI Arrests Brooklyn Man for Possession and Sale of Scarce Medical Equipment

© gettechnical inc 2021

Case Studies[71]

Medical-Related Frauds, Including

Fraudulent Cures, Tests, Vaccines, and Services [72]

U.S. Authorities Take Action Against Fraudulent COVID-19 Tests and Treatments On March 12, 2020, CBP officers at Los Angeles International Airport (LAX) intercepted a package containing suspected counterfeit or fraudulent COVID-19 test kits arriving from the United Kingdom (U.K.). The officers found six plastic bags containing various vials manifested as "Purified Water Vials," and filled with a white liquid labeled as "Corona Virus 2019nconv (COVID-19)" and "Virus1 Test Kit." [73]

The seizure triggered a joint U.S.-U.K. investigation and additional seizures.[74]

In a separate case, DOJ charged and arrested a U.K. national for shipping from the U.K. to California and Utah mislabeled drugs purported to be a COVID-19 treatment. In the scheme, the fraudster created packages labeled "Trinity COVID-19 SARS Antipathogenic Treatment" kits, even though the kits had not been approved by the FDA to treat COVID-19 or for any other use. This matter was investigated jointly by the FDA's Office of Criminal Investigation and Homeland Security Investigations, with assistance from CBP and the United States Postal Inspection Service.[75]

---

[71] *See* Financial Action Tasks (FATF) publication, "COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses," (May 2020), which identifies FATF countries' challenges, good practices, and policy responses to money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 pandemic.

[72] Other U.S. law enforcement actions include COVID-19-related arrests made by the law enforcement partners of the National Intellectual Property Rights Coordination Center (IPR Center). These arrests related to shipping mislabeled and unapproved "treatments" for patients suffering from COVID-19. *See* IPR Center Newsroom, DOJ Press Release, "U.K. National Charged with Shipping Mislabeled and Unapproved 'Treatments' for Patients Suffering from COVID-19," (April 1, 2020), and FDA, "Coronavirus Disease 2019 (COVID-19)." During a weeklong operation held March 3-10, 2020, INTERPOL, the World Customs Organization (WCO), and Europol, in collaboration with United States and partners, seized more than 37,000 counterfeit medical devices, counterfeit surgical masks, and illicit pharmaceuticals, and they identified more than 2,000 websites with false advertisements and online marketplaces selling counterfeit goods. *See* INTERPOL News, "Global operation sees a rise in fake medical products related to COVID-19," (March 19, 2020), and WCO Newsroom, "COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment," (March 23, 2020).

[73] *See* CBP National Media Release, "CBP Officers Seize Fake COVID-19 Test Kits at LAX," (March 14, 2020).

[74] *See* WCO Newsroom, "COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment," (March 23, 2020).

[75] 14. *See* DOJ Press Release, "U.K. National Charged with Shipping Mislabeled and Unapproved 'Treatments' for Patients Suffering from COVID-19," (April 1, 2020).

© gettechnical inc 2021

Non-Delivery Fraud Scams

A Virginia Financial Institution Alerted the U.S. Secret Service (USSS) and Successfully Helped Prevent a $317 Million Non-Delivery Scam

A foreign government contacted a reliable New York-based law firm for help procuring 30-50 million N95 masks for the foreign country's national police department. The New York firm reached out to a healthcare/telemedicine telemarketing company (Company A), which in turn reached out to Company B, purportedly representing "a conglomerate of doctors" that had purchased millions of masks. Company B supplied Company A with contracts falsely claiming that Company B had 50 million masks stored in a warehouse in Houston, Texas, and requiring a payment of $317 million into an escrow account.

To execute the transactions, the foreign government sent $317 million to New York for further transfer to Company A's account held at a Virginia financial institution. The Virginia financial institution became suspicious that Company A's account had only been opened the previous day, and the account owner never mentioned to the financial institution that the owner was expecting a $317 million wire transaction. The Virginia financial institution contacted the USSS.

The USSS reviewed BSA data and interviewed the accountholder for Company A. The investigation revealed that, although Company A had suspicions about Company B, Company A appeared to be a victim, hired as a "broker" for the $317 million non-delivery scam. USSS interviewed the Chief Executive Officer (CEO) of Company B who admitted that there were no masks and that he never had possession of 50 million masks.

Price Gouging and Hoarding of Medical-Related Items

FBI Arrests Brooklyn Man for Possession and Sale of Scarce Medical Equipment On March 30, 2020, FBI agents arrested a resident of Brooklyn, New York, for lying to them about his hoarding and sale of surgical masks, medical gowns, and other medical supplies.[76]

The individual allegedly sold certain designated materials, including N95 respirators, to doctors and nurses at inflated prices. In one instance, a doctor in New Jersey contacted the individual via a WhatsApp chat group labeled "Virus2020!" The individual agreed to sell to the doctor approximately 1,000 N95 masks and other assorted materials for $12,000, an approximately 700 percent markup from the normal price charged for those materials. The individual directed the doctor to an auto repair shop in Irvington, New Jersey, to pick up the order. According to the doctor, the repair shop contained enough materials, including hand sanitizers, disinfecting products, chemical cleaning supply agents, and surgical

[76] *See* DOJ Press Release, "Brooklyn Man Arrested for Assaulting FBI Agents and Making False Statements About His Possession and Sale of Scarce Medical Equipment," (March 30, 2020).

supplies, to outfit an entire hospital. In another instance, the individual allegedly offered to sell surgical gowns to a nurse and directed the nurse to his residence in Brooklyn.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying possible financial crimes related to the COVID-19 pandemic, as well as unrelated frauds and financial crimes associated with foreign and domestic political corruption, money laundering, terrorist financing, and other illicit finance. Financial institutions should provide all pertinent available information in the SAR form and narrative. Adherence to the filing instructions below will improve FinCEN and law enforcement's ability to effectively identify and pull actionable SARs and information from the FinCEN Query systems to support COVID-19-related cases.

• FinCEN requests that financial institutions reference this advisory by including the **key term "COVID19 FIN-2020-A002**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

• Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., Product Fraud – non delivery scam) in SAR field 34(z).

• Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19) May 18 Notice Related to COVID-19, which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

© gettechnical inc 2021

Financial Crimes Enforcement Network
U.S. Department of the Treasury

Paycheck Protection Program
Frequently Asked Questions (FAQs)

As of April 13, 2020

The Small Business Administration (SBA), in consultation with the U.S. Department of the Treasury, has been issuing FAQs[77] regarding implementation of the Paycheck Protection Program (PPP), established by section 1102 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act or the Act). Specifically, some of those FAQs involve explaining the requirements under the Bank Secrecy Act (BSA), and how lenders can meet those requirements when issuing a PPP loan. As the administrator of the BSA, the Financial Crimes Enforcement Network (FinCEN) is re-publishing those FAQs in this document. FinCEN will update this document with any additional BSA-related FAQs involving the PPP.As stated in the FAQs issued by the SBA, borrowers and lenders may rely on the guidance provided in this document as SBA's interpretation of the CARES Act and of the PPP Interim Final Rule ("PPP Interim Final Rule") (link). The U.S. government will not challenge lender PPP actions that conform to this guidance, and to the PPP Interim Final Rule and any subsequent rulemaking in effect at the time.[78]

1. **Question: Are PPP loans for existing customers considered new accounts for FinCEN Rule CDD purposes? Are lenders required to collect, certify, or verify beneficial ownership information in accordance with the rule requirements for existing customers?**

   Answer: If the PPP loan is being made to an existing customer and the necessary information was previously verified, you do not need to re-verify the information.

   Furthermore, if federally insured depository institutions and federally insured credit unions eligible to participate in the PPP program have not yet collected beneficial ownership information on existing customers, such institutions do not need to collect and verify beneficial ownership information for those customers applying

[77] *See* https://home.treasury.gov/policy-issues/cares/assistance-for-small-businesses.
[78] This document does not carry the force and effect of law independent of the statute and regulations on which it is based.

© gettechnical inc 2021

for new PPP loans, unless otherwise indicated by the lender's risk-based approach to BSA compliance.[79] [April 6, 2020]

2. **Question: Does the information lenders are required to collect from PPP applicants regarding every owner who has a 20% or greater ownership stake in the applicant business (i.e., owner name, title, ownership %, TIN, and address) satisfy a lender's obligation to collect beneficial ownership information (which has a 25% ownership threshold) under the Bank Secrecy Act?**
   Answer: For lenders with existing customers: With respect to collecting beneficial ownership information for owners holding a 20% or greater ownership interest, if the PPP loan is being made to an existing customer and the lender previously verified the necessary information, the lender does not need to re-verify the information. Furthermore, if federally insured depository institutions and federally insured credit unions eligible to participate in the PPP program have not yet collected such beneficial ownership information on existing customers, such institutions do not need to collect and verify beneficial ownership information for those customers applying for new PPP loans, unless otherwise indicated by the lender's risk-based approach to Bank Secrecy Act (BSA) compliance.
   For lenders with new customers: For new customers, the lender's collection of the following information from all natural persons with a 20% or greater ownership stake in the applicant business will be deemed to satisfy applicable BSA requirements and FinCEN regulations governing the collection of beneficial ownership information: owner name, title, ownership %, TIN, address, and date of birth. If any ownership interest of 20% or greater in the applicant business belongs to a business or other legal entity, lenders will need to collect appropriate beneficial ownership information for that entity. If you have questions about requirements related to beneficial ownership, go to https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule. Decisions regarding further verification of beneficial ownership information collected from new customers should be made pursuant to the lender's risk-based approach to BSA compliance.[80] [April 13, 2020]

[79] This FAQ is the same as FAQ 18 of the SBA FAQs (https://home.treasury.gov/policy-issues/cares/assistance-for-small-businesses).
[80] This FAQ is the same as FAQ 25 of the SBA FAQs (https://home.treasury.gov/policy-issues/cares/assistance-for-small-businesses).

The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic

Immediate Release
April 03, 2020
This notice updates the Financial Crimes Enforcement Network's (FinCEN's) March 16, 2020 COVID-19 Notice,[81] provides additional information to assist financial institutions in complying with their Bank Secrecy Act (BSA) obligations during the COVID-19 pandemic, and announces a direct contact mechanism for urgent COVID-19-related issues. FinCEN recognizes financial institutions face challenges related to the COVID-19 pandemic. In addition, FinCEN is committed to promoting the success of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), including the need to facilitate expeditious disbursal of CARES Act funds. Accordingly, FinCEN will issue further information, as appropriate, as the CARES Act is implemented and questions arise.

Compliance with BSA Obligations

Compliance with the Bank Secrecy Act (BSA) remains crucial to protecting our national security by combating money laundering and related crimes, including terrorism and its financing. FinCEN expects financial institutions to continue following a risk-based approach, and to diligently adhere to their BSA obligations. FinCEN also appreciates that financial institutions are taking actions to protect employees, their families, and others in response to the COVID-19 pandemic, which has created challenges in meeting certain BSA obligations, including the timing requirements for certain BSA report filings. FinCEN will continue outreach to regulatory partners and financial institutions to ensure risk-based compliance with the BSA, and FinCEN will issue additional new information as appropriate.

Beneficial Ownership Information Collection Requirements for Existing Customers

One of the primary components of the CARES Act is the Paycheck Protection Program (PPP). For eligible federally insured depository institutions and federally insured credit unions, PPP loans for existing customers will not require re-verification under applicable BSA requirements, unless otherwise indicated by the institution's risk-based approach to BSA compliance.

[81] FinCEN's March 16 COVID-19 Notice: https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions

© gettechnical inc 2021

For non-PPP loans, FinCEN reminds financial institutions of FinCEN's September 7, 2018 ruling (FIN-2018-R004) offering certain exceptive relief to beneficial ownership requirements. To the extent that renewal, modification, restructuring, or extension for existing legal entity customers falls outside of the scope of that ruling, FinCEN recognizes that a risk-based approach taken by financial institutions may result in reasonable delays in compliance.

FinCEN will continue to assess reasonable risk-based approaches to BSA obligations and will issue further information, as appropriate, particularly as the CARES Act is implemented.

BSA Reporting Obligations & Updates to Currency Transaction Report (CTR) Filing Obligations

FinCEN has heard from certain financial institutions and trade associations for financial institutions about difficulties in meeting certain BSA obligations, including the timing requirements for certain BSA report filings. In response to concerns regarding certain timing requirements of BSA filings, FinCEN recognizes that certain regulatory timing requirements with regard to BSA filings may be challenging during the COVID-19 pandemic and that there may be some reasonable delays in compliance.

FinCEN hereby suspends implementation of the February 6, 2020 ruling (FIN-2020-R001) on CTR filing obligations when reporting transactions involving sole proprietorships and entities operating under a "doing business as" (DBA) name (the "2020 Ruling") until further notice. FinCEN will issue further information on these types of CTR filings at an appropriate time with reasonable implementation periods. Until such issuance, financial institutions should continue to report transactions involving sole proprietorships and DBAs under prior practice. Those financial institutions that have already made the necessary changes to comply with the 2020 Ruling need not revert to prior practice, and may report CTRs in accordance with the now-suspended ruling.

New FinCEN COVID-19 Online Contact Mechanism

FinCEN has created a COVID-19-specific online contact mechanism, via a specific drop-down category, for financial institutions to communicate to FinCEN COVID-19-related concerns while adhering to their BSA obligations. Financial institutions that wish to communicate such COVID-19-related concerns to FinCEN must go to www.FinCEN.gov, click on "Need Assistance," and select "COVID19" in the subject drop-down list.[82] Such COVID-19-related communications are strongly encouraged but not required. FinCEN will review COVID-19-related communications. Depending on the volume of such communications, however, FinCEN may only respond via an automated message confirming receipt to communications regarding delays in filing of BSA reports due to COVID-19. FinCEN also encourages financial institutions to contact their functional regulator(s) or other BSA examining authority as soon as practicable if a financial institution has BSA compliance concerns because of the COVID-19 pandemic.[83] Financial institutions are encouraged to keep FinCEN and their functional regulator(s) or other BSA examining authority informed as their circumstances change.

[82] FinCEN's Regulatory Support Section will continue to be available to support financial institutions for the duration of the COVID-19 pandemic.

[83] COVID-19 communications to FinCEN are in addition to, and do not supersede, any methods suggested for financial institutions to communicate COVID19-related concerns to their functional regulator or BSA examining authority.

Encouragement of Innovative Efforts and Other Reminders

FinCEN encourages financial institutions to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their BSA/anti-money laundering compliance obligations, in order to further strengthen the financial system against illicit financial activity and other related fraud. Furthermore, FinCEN reminds financial institutions of the December 3, 2018 Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration, and the Office of the Comptroller of the Currency.[84]

As noted in its March 16 COVID-19 Notice, FinCEN reminds financial institutions to review information from other relevant functional regulators as updates become available. FinCEN's March 16 COVID-19 Notice alerted financial institutions to imposter scams, investment scams, product scams, and insider trading. FinCEN also advised financial institutions to remain alert for malicious or fraudulent transactions similar to those that occur in the wake of natural disasters, such as those described in FinCEN's advisory, FIN-2017-A007, "Advisory to Financial Institutions Regarding Disaster-Related Fraud" (October 31, 2017), including benefits fraud, charities fraud, and cyber-related fraud.[85] FinCEN will continue to monitor the COVID-19 National Emergency and will release updated information for financial institutions as appropriate.

[84] Joint Statement on Innovation Efforts: https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf

[85] FIN-2017-A007 - Advisory to Financial Institutions Regarding Disaster-Related Fraud (October 31, 2017): https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf

© gettechnical inc 2021

The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity

Immediate Release
March 16, 2020
On March 13, 2020, President Trump declared a National Emergency in response to COVID-19.[86] FinCEN requests financial institutions affected by the COVID-19 pandemic to contact FinCEN and their functional regulator as soon as practicable if a COVID-19-affected financial institution has concern about any potential delays in its ability to file required Bank Secrecy Act (BSA) reports. Financial institutions seeking to contact FinCEN should call FinCEN's Regulatory Support Section (RSS) at 1-800-949-2732 and select option 6 or e-mail at FRC@fincen.gov. FinCEN's RSS will continue to be available to support financial institutions for the duration of the COVID-19 pandemic.

Financial institutions are encouraged to keep FinCEN and their functional regulators informed as their circumstances change.

FinCEN also advises financial institutions to remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters. FinCEN is monitoring public reports and BSA reports of potential illicit behavior connected to COVID-19 and notes the following emerging trends:

1. Imposter Scams – Bad actors attempt to solicit donations, steal personal information, or distribute malware by impersonating government agencies (e.g., Centers for Disease Control and Prevention), international organizations (e.g., World Health Organization (WHO)[87]), or healthcare organizations.
2. Investment Scams – The U.S. Securities and Exchange Commission (SEC) urged investors to be wary of COVID-19-related investment scams, such as promotions that

[86] Remarks by President Trump, Vice President Pence, and Members of the Coronavirus Task Force in Press Conference: https://www.whitehouse.gov/briefings-statements/remarks-president-trump-vice-president-pence-members-coronavirus-task-force-press-conference-3/
[87] WHO statement concerning imposter scams: https://www.who.int/about/communications/cyber-security

© gettechnical inc 2021

falsely claim that the products or services of publicly traded companies can prevent, detect, or cure coronavirus.[88]

3. Product Scams – The U.S. Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19.[89] Additionally, FinCEN has received reports regarding fraudulent marketing of COVID-19-related supplies, such as certain facemasks.
4. Insider Trading – FinCEN has received reports regarding suspected COVID-19-related insider trading.

In addition, please see FinCEN's advisory, FIN-2017-A007 "Advisory to Financial Institutions Regarding Disaster-Related Fraud" (October 31, 2017) for descriptions of other relevant typologies, such as benefits fraud, charities fraud, and cyber-related fraud.[90] For suspected suspicious transactions linked to COVID-19, along with checking the appropriate suspicious activity report-template (SAR-template) box(es) for certain typologies, FinCEN also encourages financial institutions to enter "COVID19" in Field 2 of the SAR-template.

Financial institutions are encouraged to review information from other relevant functional regulators as updates are available. FinCEN will continue to monitor this situation and will release updated information for financial institutions as appropriate.

[88] SEC Notice on COVID-19 related investment scams: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus

[89] FTC and FDA joint updated statement concerning product scams: https://www.consumer.ftc.gov/blog/2020/03/ftc-fda-warnings-sent-sellers-scam-coronavirus-treatments

[90] FIN-2017-A007- Advisory to Financial Institutions Regarding Disaster-Related Fraud (October 31, 2017): https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf

© gettechnical inc 2021

© gettechnical inc 2021