

FinCEN Advisory Cheatsheet



COMPLIANCE COHORT

Copyright 2023 by Compliance Cohort, LLC

We are not attorneys. Seek legal counsel.

Unauthorized Duplication Prohibited

All Rights Reserved

www.compliancecohort.com

Topic: Human Smuggling on the U.S. Southwest Border

Alert Name: FinCEN Alert on Human Smuggling along the Southwest Border of the United States

Alert Date: 1/13/2023

Alert Number: FIN-2023-Alert001

Alert Link:

- https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf

Applicable SAR Instructions:

- FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this alert by including the key term “FIN-2023-HUMANSMUGGLING” in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative, and by selecting SAR field 38(g) (human smuggling)
- Financial institutions that suspect human trafficking activity should also select SAR field 38(h) (human trafficking) and highlight other advisory or alert keywords in the narrative, if applicable
- Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity.
- Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.

Topic: Potential Russian and Belarusian Export Control Evasion Attempts

Alert Name: FinCEN and the U.S. Department of Commerce’s Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts

Alert Date: 6/28/2022

Alert Number: FIN-2022-Alert003

Alert Link:

- <https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this alert by including the key term “FIN2022-RUSSIABIS” 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 alert. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

- FinCEN also requests that financial institutions check box 38(z) (Other Suspicious Activity) and note “Russia Export Restrictions Evasion”.
- If known, please also indicate in field 45(z) (Other Product Types) the appropriate North American Industry Code(s) (NAICs) for the involved product, and/or the appropriate financial instrument or payment mechanism in field 46.
- Financial institutions should include any and all available information relating to the products or services involved in the suspicious activity, including all available transportation and trade financing documentation, accounts and locations involved, identifying information and descriptions of any legal entities or arrangements involved or associated with beneficial owners, and any information about related persons or entities (including transportation companies or services) involved in the activity.

Topic: Elder Financial Exploitation

Advisory Name: Advisory on Elder Financial Exploitation

Advisory Date: 6/15/2022

Advisory Number: FIN-2022-A002

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf>

Applicable SAR Instructions:

- When filing a SAR, financial institutions should provide all pertinent available information about the activity in the SAR form and narrative. Reporting on how perpetrators of EFE communicate with and target older adults is also useful to law enforcement investigations.
- FinCEN requests that financial institutions reference this advisory by including the key term “EFE FIN-2022-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 that suspect EFE activity should also mark the check box for Elder Financial Exploitation (SAR Field 38(d)).
- Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity.
- Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.

Topic: Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members

Alert Name: FinCEN Alert on Real Estate, Luxury Goods, and Other HighValue Assets Involving Russian Elites, Oligarchs, and their Family Members

Alert Date: 3/16/2022

Alert Number: FIN-2022-Alert002

Alert Link:

- https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Elite%20High%20Value%20Assets_508%20FINAL.pdf

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this alert by including the key term “FIN-2022-RUSSIASANCTIONS” 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 alert. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.
- Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the FinCEN Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).
- Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.

Topic: Potential Russian Sanctions Evasion Attempts

Alert Name: FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts

Alert Date: 3/7/2022

Alert Number: FIN-2022-Alert001

Alert Link:

- <https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this alert by including the key term “FIN-2022-RUSSIASANCTIONS” 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 alert.

- Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the FinCEN Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).
- It is critical that financial institutions (including CVC exchanges) identify and immediately report any suspicious transactions associated with ransomware attacks. For purposes of meeting a financial institution's SAR obligations, FinCEN and law enforcement consider suspicious transactions involving ransomware attacks to constitute "situations involving violations that require immediate attention."
- Financial institutions must subsequently file a SAR using FinCEN's BSA E-filing System, providing as much of the relevant details around the activity as available at that time. Amended SARs should be filed to include additional information related to the same activity that is learned later; completely new activity should be filed in a new "initial" SAR filing.
- Financial institutions also should include any relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields (42-44) on the SAR. Any data or information that helps identify the activity as suspicious can be included as an indicator. Examples include chat logs, suspicious IP addresses, suspicious email addresses, suspicious filenames, malware hashes, CVC addresses, command and control (C2) IP addresses, C2 domains, targeted systems, MAC address or port numbers.

Topic: Environmental Crimes and Related Financial Activity

Notice Name: FinCEN Calls Attention to Environmental Crimes and Related Financial Activity

Notice Date: 11/18/2021

Notice Number: FIN-2021-NTC4

Notice Link:

- <https://www.fincen.gov/sites/default/files/2021-11/FinCEN%20Environmental%20Crimes%20Notice%20508%20FINAL.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference only this notice in SAR field 2 (Filing Institution Note to FinCEN) using keyword "FIN-2021-NTC4;" this keyword should also be referenced in the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.
- Financial institutions should also select SAR field 38(z) (Other Suspicious Activities - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and environmental crimes and use the most relevant keyword for suspicious activity such as "wildlife trafficking," "illegal logging," "illegal fishing," "illegal mining," or "waste trafficking." If the suspicious activity involves multiple potential offenses, FinCEN also requests that filers include all relevant keywords in the narrative.

- Financial institutions may consider sharing information on suspected environmental crimes offenses under Section 314(b) for the purposes of identifying and reporting money laundering activity.
- On the SAR Narrative, FinCEN also requests that filers further detail how the suspicious activity relates to environmental crimes. Filers should provide any available details concerning how the illicit product, plant, or waste was solicited, acquired, stored, transported, financed, and paid for.
- Filers also should provide all available details (such as names, identifiers, and contact information— including Internet Protocol (IP) and email addresses and phone numbers) regarding: (i) any actual purchasers or sellers of the illicit product, plant, waste or waste disposal services, and their intermediaries or agents; (ii) the volume and dollar amount of the transactions involving an entity that is—or may be functioning as—a supplier of illicit products, plants, waste or waste services; and (iii) any beneficial owner(s) of involved entities (such as shell companies).
- In the case of illicit waste, filers should provide all available details and specific descriptions of the waste product and any known details about its origin, transport, and destination.
- If known, filers should provide information about the place(s) where the reported individuals or entities are operating.

Topic: Ransomware and Ransom Payments

Advisory Name: Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Advisory Date: 11/08/2021

Advisory Number: FIN-2021-A004

Advisory Link:

- https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this advisory by including the key term “CYBER-FIN-2021-A004” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and ransomware-related activity.
- Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including “ransomware” as keywords in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity.
- Additionally, financial institutions should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

Topic: Online Child Sexual Exploitation

Notice Name: FinCEN Calls Attention to Online Child Sexual Exploitation Crimes

Notice Date: 09/16/2021

Notice Number: FIN-2021-NTC3

Notice Link:

- <https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference only this notice in SAR field 2 (Filing Institution Note to FinCEN) using the keyword “OCSE-FIN-2021-NTC3”; this keyword should also be referenced in the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice. Financial institutions may highlight additional advisory keywords in the narrative, if applicable.
- Financial institutions should also select SAR Field 38(z) (Other) as the associated suspicious activity type to indicate a connection between the suspicious activity reported and OCSE activity and include the term “OCSE” in the text box. If known, enter the subject’s internet based contact with the financial institution in SAR Field 43 (IP Address and Date).
- If human trafficking or human smuggling are suspected in addition to OCSE activity, financial institutions should also select SAR Field 38(h) (Human Trafficking) or SAR Field 38(g) (Human Smuggling), respectively.
- FinCEN asks that reporting entities use the Child Sexual Exploitation (CSE) terms and definitions in the appendix of the Advisory when describing suspicious activity, which will assist FinCEN’s analysis of the SARs.
- For additional information on reporting cyber-enabled crimes, including on how to file SARs, please see: [FAQs for Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information](#). Collaboration between Bank Secrecy Act (BSA)/anti-money-laundering (AML) and cybersecurity units within financial institutions is an effective practice for gathering information helpful to identifying OCSE offenders and victims. Please refer to [FinCEN’s Advisory on Cyber-Events and Cyber-Enabled Crime](#), which contains examples of useful information to report including chat logs, IP addresses, email addresses, filenames, and CVC addresses, such as bitcoin. Financial institutions may consider sharing cyber-related information for the purposes of identifying and reporting money laundering and OCSE offenses.

Topic: Updated Deficient Countries

Advisory Name: Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies

Advisory Date: 03/11/2021

Advisory Number: FIN-2021-A003

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2021-03-11/FATF%20February%202021%20Advisory%20FINAL%20508.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this advisory by including the key term “FATF FIN-2021-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.

Topic: Trade in Antiquities and Art

Notice Name: FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art

Notice Date: 03/09/2021

Notice Number: FIN-2021-NTC2

Notice Link:

- https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20Notice%20on%20Antiquities%20and%20Art_508C.pdf

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference “FIN-2021-NTC2” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.
- Financial institutions should also select SAR field 36(z) (Money Laundering - other) as the associated suspicious activity type, and note if the suspicious activity relates to “Antiquities,” “Art,” or both (in some instances, an object could be considered both an antiquity and a work of art).
- FinCEN also requests that filers detail the reported activity in the narrative portion of the SAR, explaining how the suspicious activity relates to “Antiquities,” “Art,” or both.
- Filers should provide any available details that may assist in the identification of (1) the objects connected to the financial transactions, (2) other transactions or proposed transactions that may involve antiquities or art, and (3) any other relevant information.
- Filers should provide all available details (such as names, identifiers, and contact information—including Internet Protocol (IP) and email addresses and phone numbers) regarding (1) the actual purchasers or sellers of the property, and their intermediaries or agents, (2) the volume and dollar amount of the transactions involving an entity that is—or may be functioning as—a dealer in antiquities or art, and (3) any beneficial owner(s) of entities (such as shell companies).
- In the case of stolen art or antiquities, filers should provide a detailed and specific description of the stolen item(s) and indicate whether photographs of the items are available.

- Filers should also provide information about the place(s) where the reported individuals or entities are operating.

Topic: COVID-19 Economic Impact Payments

Advisory Name: Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments

Advisory Date: 02/24/2021

Advisory Number: FIN-2021-A002

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2021-02-24/Advisory%20EIP%20FINAL%20508.pdf>

Applicable SAR Instructions:

- Use the key term “FIN-2021-A002” 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.
- FinCEN also requests that filers mention “economic impact payment” in the SAR narrative along with any other relevant behavior, such as counterfeit checks, money mule activity, or identity theft, to indicate a connection between those activities and EIP frauds and thefts. Additionally, FinCEN requests that filers use this program-specific term and avoid relying on generalized key terms, such as “stimulus check.”
- 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., economic impact payment) in SAR field 34(z).
- FinCEN requests filers not report the potential victim of an EIP fraud scheme as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.
- Please refer to FinCEN’s [May 2020 Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#) and [February 2021 Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions](#), which contain information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

Topic: COVID-19 Health Care and Insurance Fraud

Advisory Name: COVID-19 Health Insurance and Health Care-Related Fraud

Advisory Date: 02/02/2021

Advisory Number: FIN-2021-A001

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2021-02-02/COVID-19%20Health%20Care%20508%20Final.pdf>

Applicable SAR Instructions:

- Use the key term “FIN-2021-A001” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR 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(g) (health care – public or private health insurance) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include additional detail about the type of health care fraud (e.g., Medicare – services not provided) in the narrative.
- FinCEN requests that financial institutions wishing to report potential health care fraud unrelated to COVID-19 should not include this advisory’s key term in SAR field 2 or the SAR’s narrative portion. Instead, please select field 34(g) and detail the activity in the narrative (e.g. addiction treatment – services not provided; or pain clinic – “marketing” fees).
- Please refer to FinCEN’s May 2020 Notice Related to the Coronavirus Disease 2019 (COVID-19) which contains information regarding reporting COVID-19-related crime, and remind financial institutions of certain BSA obligations.
 - Link: https://www.fincen.gov/sites/default/files/shared/May_18_Notice_Related_to_COVID-19.pdf

Topic: COVID-19 Vaccine Related Scams

Notice Name: FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks

Notice Date: 12/28/2020

Notice Number: FIN-2020-NTC4

Notice Link:

- <https://www.fincen.gov/sites/default/files/shared/COVID-19%20Vaccine%20Notice%20508.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference “FIN-2020-NTC4” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.
- 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., vaccine scam or vaccine ransomware) in SAR field 34(z).
- FinCEN requests that filers further detail the reported activity in the narrative portion of the SAR. If the activity is suspected of being a scam, filers should provide known details about how the scammers contacted the victim, how the victim provided or attempted to provide payment related to the scam, and any other available details including data

related to the financial transactions or method of contact, such as Internet Protocol (IP) addresses and phone numbers. For guidance on ransomware attacks, see FinCEN Advisory, FIN-2020-A006, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” (October 1, 2020).

- Link:
<https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>
- Please refer to FinCEN’s May 2020 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.
 - Link:
https://www.fincen.gov/sites/default/files/shared/May_18_Notice_Related_to_COVID-19.pdf

Topic: FATF Identified Deficient Jurisdictions

Advisory Name: Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Deficiencies

Advisory Date: 11/06/2020

Advisory Number: FIN-2020-A009

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2020-11-06/FATF%20October%202020%20Advisory%20FINAL%20508.pdf>

Applicable SAR Instructions:

- Use the key term “October 2020 FATF FIN-2020-A009” 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.

Topic: Human Trafficking and Related Activity

Advisory Name: Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity

Advisory Date: 10/15/2020

Advisory Number: FIN-2020-A008

Advisory Link:

- https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf

Applicable SAR Instructions:

- A potential victim of human trafficking should not be reported as the subject of a SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

- Use the key term: “HUMAN TRAFFICKING FIN-2020-A008” in SAR field 2 (Filing Institution Note to FinCEN) to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Additional information to include behavioral indicators, email addresses, phone numbers, and IP addresses also should be included when possible to aid law enforcement investigations.

Topic: COVID-19 Unemployment Insurance Fraud

Advisory Name: Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic

Advisory Date: 10/13/2020

Advisory Number: FIN-2020-A007

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2020-10-13/Advisory%20Unemployment%20Insurance%20COVID%2019%20508%20Final.pdf>

Applicable SAR Instructions:

- Use 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 SAR, financial institutions should include the keywords “unemployment fraud” 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.
 - Link: https://www.fincen.gov/sites/default/files/shared/May_18_Note_Related_to_COVID-19.pdf

Topic: Ransomware and Ransom Payments

Advisory Name: Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Advisory Date: 10/01/2020

Advisory Number: FIN-2020-A006

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>

Applicable SAR Instructions:

- Use the key term: “CYBER-FIN-2020-A006” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and ransomware-related activity.
- Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including “ransomware” as keywords in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity.
- Additionally, financial institutions should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)- (j), (z).

Topic: COVID-19 Cybercrime and Cyber-Enabled Crime

Advisory Name: Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic

Advisory Date: 7/30/2020

Advisory Number: FIN-2020-A005

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf>

Applicable SAR Instructions:

- Use 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.”
- 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 fields 42a and 42z (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.
 - Link:
https://www.fincen.gov/sites/default/files/shared/May_18_Notice_Related_to_COVID-19.pdf

Topic: Convertible Virtual Currency Scam Involving Twitter

Alert Name: FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter

Alert Date: 7/16/2020

Alert Number: FIN-2020-Alert001

Alert Link:

- https://www.fincen.gov/sites/default/files/2020-07/FinCEN%20Alert%20Twitter_508%20FINAL.pdf

Applicable SAR Instructions:

- Use the key term "FIN-2020-Alert001" 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 alert.

Topic: COVID-19 Imposter Scams and Money Mule Schemes

Advisory Name: Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)

Advisory Date: 7/7/2020

Advisory Number: FIN-2020-A003

Advisory Link:

- https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf

Applicable SAR Instructions:

- Use 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 field 34(l) (Fraud-Massmarketing), 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.
 - Link:
https://www.fincen.gov/sites/default/files/shared/May_18_Notice_Related_to_COVID-19.pdf

Topic: Medical Scams Related to Coronavirus Disease 2019

Advisory Name: Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)

Advisory Date: 5/18/20

Advisory Number: FIN-2020-A002

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf>

Applicable SAR Instructions:

- 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.
 - https://www.fincen.gov/sites/default/files/shared/May_18_Notice_Related_to_COVID-19.pdf

Topic: Fentanyl & Other Synthetic Opioids

Advisory Name: Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids

Advisory Date: 8/21/2019

Advisory Number: FIN-2019-A006

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf>

Applicable SAR Instructions:

- When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. FinCEN requests that financial institutions use only the updated mandatory SAR form (as of February 1, 2019) and reference this advisory using the following key term in SAR field 2 (Filing Institution Note to FinCEN): “FENTANYL FIN-2019-A006” to indicate a possible connection between the suspicious activities being reported and activities highlighted in this advisory.

Topic: Updated Email Compromise Fraud Schemes

Advisory Name: Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes

Advisory Date: 7/16/2019

Advisory Number: FIN-2019-A005

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this advisory and include the following key terms in the SAR narrative: “BEC FRAUD” when businesses or organizations are the scheme victims “EAC FRAUD” when individuals are the scheme victims Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type 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. Additionally, financial institutions should include any relevant technical cyber indicators related to the email compromise fraud and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z). In instances of reporting of BEC schemes that result in the communication of information that could be used to facilitate future fraudulent transactions, which may be voluntary, FinCEN requests that financial institutions include the following key term in the SAR narrative: “BEC DATA THEFT”
- NOTE: There is a large amount of info in the advisory that FinCEN states would be useful to include in each SAR on this topic.

Topic: Convertible Virtual Currency

Advisory Name: Advisory on Illicit Activity Involving COnvertible Virtual Currency

Advisory Date: 5/9/19

Advisory Number: FIN-2019-A003

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>

Applicable SAR Instructions:

- FinCEN requests that financial institutions reference this advisory by including the key term: “CVC FIN-2019-A003” in the SAR narrative to indicate a connection between the suspicious activity being reported and possible illicit activity involving CVC. Using the new, mandatory SAR Form that took effect on January 1, 2019, financial institutions should reference this advisory using the above key term in SAR field 2 (“Filing Institution Note to FinCEN”)

Topic: Venezuela Corruption

Advisory Name: Updated Advisory on Widespread Public Corruption in Venezuela

Advisory Date: 5/3/19

Advisory Number: FIN-2019-A002

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2019-05-08/Venezuela%20Advisory%20FINAL%20508.pdf>

Applicable SAR Instructions:

- When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. FinCEN requests financial institutions only use the updated mandatory SAR form (as of February 1, 2019). FinCEN further requests that financial institutions select SAR field 38(m) (“Suspected Public/Private Corruption (Foreign)”) and reference this advisory by including the key term: “Venezuela Corruption FIN-2019-A002” in SAR field 2 (“Filing Institution Note to FinCEN”) to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in this advisory.

Topic: Iranian Activities

Advisory Name: Advisory on the Iranian Regime’s Illicit and Malign Activities and Attempts to Exploit the Financial System

Advisory Date: 10/11/2018

Advisory Number: FIN-2018-A006

Advisory Link:

- <https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf>

Applicable SAR 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 reference this advisory by including the key term: “Iran FIN-2018-A006” to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in this advisory.

Topic: Nicaragua Corruption

Advisory Name: Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua

Advisory Date: 10/4/18

Advisory Number: FIN-2018-A005

Advisory Link:

- https://www.fincen.gov/sites/default/files/advisory/2018-10-04/Nicaragua_Advisory_FINA_L_508_0.pdf

Applicable SAR 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: "Nicaragua FIN-2018-A005" in the SAR narrative and in SAR field 35(z) ("Other Suspicious Activity-Other") when using the SAR Form on or prior to December 31, 2018. Beginning January 1, 2019, when using the new, mandatory SAR Form, financial institutions should select SAR field 38(m) ("Suspected Public/Private Corruption (Foreign)") and reference this advisory using the above key term in SAR field 2 ("Filing Institution Note to FinCEN") to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in this advisory.

Topic: Corrupt Foreign PEPs

Advisory Name: Advisory on Human Rights Abuses Enabled by Corrupt Senior Political Figures and their Financial Facilitators

Advisory Date: 6/12/18

Advisory Number: FIN-2018-A003

Advisory Link:

- <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-a003>

Applicable SAR Instructions:

- See FIN-2008-G005
- When filing, select SAR field 35(l) and include term "Financial Facilitator FIN-2018-A003" in SAR narrative and in SAR field 35(z)
- If transactions may potentially relate to a terrorist activity, call the FI Hotline at 866-556-3974 to expedite delivery of said information.

Things to look for:

- Use of third parties when it is not normal business practice
- Use of third parties when it appears to shield the identity of a PEP
- Use of family members or close associates as legal owners
- Use of corporate vehicles (legal entities and legal arrangements) to obscure ownership, involved industries, and/or countries

- Declarations of information from PEPs that are inconsistent with other information, such as publicly available asset declarations and published official salaries
- The PEP or facilitator seeks to make use of the services of a financial institution or a designated non-financial business or profession (DNFBP) that would normally not cater to foreign or high-value clients
- The PEP or facilitator repeatedly moves funds to and from countries with which the PEP does not appear to have ties
- The PEP or facilitator has a substantial authority over or access to state assets and funds, policies, and operations
- The PEP or facilitator has an ownership interest in or otherwise controls the financial institution of DNFBP (either privately or ex officio) that is a counterparty or a correspondent in a transaction
- 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)
- 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
- 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)
- Payments involving government contracts that originate from third parties that are not official government entities (e.g., shell corporations)
- Transactions involving property or assets expropriated or otherwise taken over by corrupt regimes, including individual senior foreign officials or their croneis

Topic: Email Compromise Fraud Schemes

Advisory Name: Advisory to Financial Institutions on Email Compromise Fraud Schemes

Advisory Date: 9/6/16

Advisory Number: FIN-2016-A003

Advisory Link:

- <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003>

Applicable SAR Instructions:

- When filing, provide all available information, including cyber-related information, in the SAR narrative. Specifically, provide the following information:
- Scheme Details
 - Dates and amounts of suspicious transactions
 - Sender’s identifying information, account number, and financial institution
 - Beneficiary’s identifying information, account number, and financial institution
 - 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
- Communication with other FI's under the auspices of Section 314(b) is encouraged by FinCEN when determining if a SAR filing is necessary
- Reference advisory FIN-2016-A003 and include the key terms "BEC Fraud" when a business is the scheme victim and/or "EAC Fraud" when an individual is the scheme victim in the SAR narrative and SAR field 31(z) to indicate a connection between the suspicious activity being reported and possible BAC or EAC fraud. Include one or both terms to the extent a distinction is able to be made.

Topic: Human Smuggling and Human Trafficking

Advisory Name: Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags

Advisory Date: 9/11/2014

Advisory Number: FIN-2014-A008

Advisory Link: <https://www.fincen.gov/sites/default/files/shared/FIN-2014-A008.pdf>

Applicable SAR Instructions:

- Include one or both of the following terms in the Narrative and Suspicious Activity Information to the extent that a distinction is able to be made.
 - Advisory Human Smuggling
 - Advisory Human Trafficking
- Include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious.
- Do not identify the potential victim of human smuggling or trafficking as the subject of the SAR. Rather, include the potential victim's information in the narrative portion of the SAR.

Topic: Funnel Accounts and TBML in Mexico; BMPE; MX

Restriction

Advisory Name: Update on US Currency Restrictions in Mexico: Funnel Accounts and TBML

Advisory Date: 5/28/14

Advisory Number: FIN-2014-A005

Advisory Link: <https://www.fincen.gov/sites/default/files/shared/FIN-2014-A005.pdf>

Applicable SAR Instructions:

- Include "MX Restriction" in SAR narrative and Suspicious Activity Information sections of SARs to indicate a possible connection between the suspicious activity being reported and the enacted US currency restrictions on Mexican financial institutions
- Include specific reference to the terms "funnel account" and/or "TBML" where appropriate.

Topic: St. Kitts and Nevis Passport

Advisory Name: Abuse of the Citizenship-by-Investment Program Sponsored by the Federation of St. Kitts and Nevis

Advisory Date: 5/20/14

Advisory Number: FIN-2014-A004

Advisory Link: <https://www.fincen.gov/sites/default/files/shared/FIN-2014-A004.pdf>

Applicable SAR Instructions:

- Include the term SKN Passport in both the narrative portion and in the “Other” fields in Part II items 29 through 38, as applicable
- Be sure to consider any OFAC obligations if they believe that customers using the SKN passports are blocked persons

Topic: Tax Refund Fraud

Advisory Name: Tax Refund Fraud and Related Identity Theft

Advisory Date: 3/30/12

Advisory Number: FIN-2012-A005

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a005>

Applicable SAR Instructions:

- Include the term “tax refund fraud” in the narrative section of the SAR and provide a detailed description of the activity

Topic: Tax Refund Fraud

Advisory Name: Update on Tax Refund Fraud and Related Identity Theft

Advisory Date: 2/26/13

Advisory Number: FIN-2013-A001

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2013-a001>

Applicable SAR Instructions:

- Include the term “tax refund fraud” in the narrative section of the SAR and provide a detailed description of the activity
- As these are time sensitive transactions, a FI may contact their local IRS Criminal Investigation Field Office to alert them that a SAR has been filed related to tax refund fraud

Topic: Third-Party Payment Processors

Advisory Name: Risk Associated with Third-Party Payment Processors

Advisory Date: 10/22/12

Advisory Number: FIN-2012-A010

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a010>

Applicable SAR Instructions:

- When reporting suspicious activity, 1) check the appropriate box on the SAR form to indicate the type of suspicious activity and 2) include the term “Payment Processor” in both the narrative portion and subject occupation portions of the SAR

Topic: Mexican Currency Restriction

Advisory Name: Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency

Advisory Date: 6/21/12

Advisory Number: FIN-2010-A007

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a007>

Applicable SAR Instructions:

- If a financial institution has determined that a transaction is suspicious and thus has an obligation to file a SAR with FinCEN; AND if the facts and circumstances of the transaction lead the financial institution to suspect that the transaction is being entered into as a result of the Mexican currency restrictions, then the financial institution should include the specific term "MX Restriction" within the narrative portion of the SAR filing and highlight the exact dollar amount(s) associated with the suspicious activity
- Include all information available for each party suspected of engaging in this activity (including the individual or company name, address, phone number, and any other identifying information)
- If currency is shipped from Mexico, include information on the common carrier, courier, or shipper of the currency, and information on the point of exportation of the currency from Mexico and the point of importation in the United States, if known

Topic: Mexican Currency Restriction

Advisory Name: Update on US Currency Restrictions in Mexico

Advisory Date: 7/18/12

Advisory Number: FIN-2012-A006

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a006>

Applicable SAR Instructions:

- Include “MX Restriction” in the narrative portion of the SAR

Topic: Account Takeover Fraud

Advisory Name: Account Takeover Activity

Advisory Date: 12/19/11

Advisory Number: FIN-2011-A016

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a016>

Applicable SAR Instructions:

- Include the term “account takeover fraud” in the narrative section of the SAR and provide a detailed description of the activity
- If the account takeover involves computer intrusion, check the box for "computer intrusion." In addition, financial institutions can check the "other" box and note "account takeover fraud" in the space provided
- If the account takeover involved other delivery channels such as telephone banking or fraudulent activities such as social engineering, financial institutions can check the "other" box, note "account takeover fraud," and include a short description of the additional information in the space provided
- If the account takeover involves a wire transfer, then in addition to selecting the "other" box and noting "account takeover fraud," the box for "wire transfer fraud" should be checked
- If the account takeover involves an ACH transfer, financial institutions can check the "other" box and note "account takeover fraud - ACH"
- Account takeovers often involve unauthorized access to PINs, account numbers, and other identifying information. Financial institutions may need to check the box for "identity theft," in addition to selecting the "other" box and noting "account takeover fraud." Additional boxes should be checked if appropriate (e.g. "terrorist financing")

Topic: Bankruptcy

Advisory Name: The US Trustee Program’s Civil Enforcement Activity Targets Bankruptcy-Related Mortgage Fraud and Mortgage Rescue Schemes (SAR Activity Review – October 2011)

Advisory Date: 10/12/11

Advisory Number: SAR Activity Review – October 2011

Advisory Link: https://www.fincen.gov/sites/default/files/shared/sar_tti_20.pdf#page=61

Topic: Commercial Real Estate Fraud (CREF)

Advisory Name: Advisory on Activities Potentially Related to CREF

Advisory Date: 3/30/11

Advisory Number: FIN-2011-A007

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a007>

Applicable SAR Instructions:

- Include the term CREF within the narrative portion of all relevant SAR filings, even though the SAR form lists “commercial loan fraud” as a check box
- Report the exact dollar amounts associated with the commercial real estate activity
- Include all information available for all parties suspected of participating in this fraudulent activity in the Suspect/Subject Information Section

Topic: Elder Financial Exploitation

Advisory Name: Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation

Advisory Date: 2/22/11

Advisory Number: FIN-2011-A003

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003>

Applicable SAR Instructions:

- Select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR
- Include the term “elder financial exploitation” in the narrative portion of all SARs filed
- Include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious in the narrative section
- The potential victim should not be reported as the subject of the SAR, but rather included in the narrative portion of the SAR

Topic: Informal Value Transfer System (IVTS)

Advisory Name: Informal Value Transfer Systems

Advisory Date: 9/1/10

Advisory Number: FIN-2010-A011

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a011>

Applicable SAR Instructions:

- File a SAR if an FI knows, suspects, or has reason to suspect that an IVTS is operating in violation of the registration requirement under the BSA for money transmitters and not acting solely as agents of others, or, even if registered, is being used in the illegal transmittal of funds
- Check the appropriate box indicating the type of suspicious activity being reported
- Note the abbreviation “IVTS” in the narrative
- Include an explanation as to why the FI knows, suspects, or has reason to suspect that an IVS may be involved in the reported activity in the narrative section of the SAR

Topic: Home Equity Conversion Mortgage (HECM)/Federal Housing Authority (FHA)

Advisory Name: Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Home Equity Conversion Mortgage Fraud Schemes

Advisory Date: 4/27/10

Advisory Number: FIN-2010-A005

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a005>

Applicable SAR Instructions:

- Provide complete and sufficient descriptions of known or suspected criminal violations or suspicious activity in the SAR narrative sections
- Include the term “HECM” within the narrative portions of all relevant SAR filings
- Highlight the exact dollar amounts associated with the HECM loan proceeds
- Include all information available for each party suspected of engaging in this fraudulent activity in the Suspect/Subject Information Section of the SAR
 - Include individual or company name, address, phone number, and any other identifying information
- If the FI is aware of any other type of FHA-insured mortgage fraud, include the term “FHA” in the narrative portions of the relevant SAR filings
- If a senior homeowner is a victim of the scam, do not include them as a suspect unless there is reason to believe the homeowner knowingly participated in the fraudulent activity
- When a senior homeowner is simply a victim of a scam, include sufficient information in the narrative portion of the SAR about the senior homeowner and his or her property to assist law enforcement in investigating and prosecuting these potential crimes

Topic: Trade Based Money Laundering (TBML); Black Market Peso Exchange (BMPE)

Advisory Name: Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering

Advisory Date: 2/18/10

Advisory Number: FIN-2010-A001

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a001>

Applicable SAR Instructions:

- Check the appropriate box in the Suspicious Activity Information section of the SAR form
- Include the abbreviation “TBML” or “BMPE” in the narrative portion of all relevant SARs filed
- Include an explanation of why the institution suspects, or has reason to suspect, that the customer is participating in this type of activity in the narrative section

Topic: SIGTARP (Special Inspector General for the Trouble Asset Relief Program)

Advisory Name: Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding TARP-related Programs

Advisory Date: 10/14/09

Advisory Number: FIN-2009-A006

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2009-a006>

Applicable SAR Instructions:

- Check the appropriate box on the SAR form to indicate the type of suspicious activity
- Include the term “SIGTARP” in the narrative portion of the SAR

- Include all information available for each party suspected of engaging in the suspicious activity in the Suspect/Subject Information Section of the SAR
 - Include information such as individual or company name, address, phone number and any other identifying information

Topic: Foreclosure Rescue Scam

Advisory Name: Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding Loan Modification/Foreclosure Rescue Scams

Advisory Date: 4/6/09

Advisory Number: FIN-2009-A001

Advisory Link:

<https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-financial-institutions-filing-suspicious-activity>

Applicable SAR Instructions:

- Provide complete and sufficient descriptions of known or suspected criminal violations or suspicious activity in the narrative section
- Include the term “foreclosure rescue scam” in the narrative portions of all relevant SARs filed
- Include all information available for each party suspected of engaging in this fraudulent activity in the Suspect/Subject Information Section of the SAR
 - Include information such as individual or company name, address, phone number and any other identifying information
- The homeowner should not be listed as a subject when they are simply a victim, but rather should have their information listed in the narrative section of the SAR
- If there is reason to believe the homeowner knowingly participated in the fraudulent activity, they should be listed in the subject section of the SAR

Topic: Foreclosure Rescue Scam

Advisory Name: Updated Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Loan Modification/Foreclosure Rescue Scams

Advisory Date: 6/17/10

Advisory Number: FIN-2010-A006

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a006>

Applicable SAR Instructions:

- Include the term “foreclosure rescue scam”
- Include all information available for each party suspected of engaging in suspected fraudulent activity
 - Include information such as individual or company name, address, phone number, and any other identifying information
- When the homeowner is believed to be simply a victim, include all available information in the narrative portion of the SAR about the homeowner and his or her property

- The homeowner should not be listed as a suspect unless there is reason to believe the homeowner knowingly participated in the fraudulent activity

Topic: Foreign Corruption

Advisory Name: Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption

Advisory Date: 4/17/08

Advisory Number: FIN-2008-G005

Advisory Link: <https://www.fincen.gov/resources/advisories/fincen-guidance-fin-2008-g005>

Applicable SAR Instructions:

- Provide a detailed description of the known or suspected criminal violation or suspicious activity in the narrative sections of SARs