

# ***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.”

### **Confidentiality of SARs:**

A FinCEN Suspicious Activity Report (FinCEN SAR), and any information that would reveal the existence of the FinCEN SAR (collectively, “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).

### **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 SAR, or any information that would reveal the existence of the 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 SAR may share the SAR, or any information that would reveal the existence of the 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 SAR regulation. The sharing of 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 SAR rule. Therefore, such sharing within the depository institution’s corporate organizational structure is consistent with the purposes of Title II of the BSA.

## **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 FinCEN SAR is based; and
- For those institutions regulated by a federal functional regulator (federal bank regulatory agencies, the SEC, and the 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 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 or 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.

## **FinCEN SAR Filing Instructions:**

**1. Who Must File:** Certain financial institutions 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 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 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.

## **FinCEN SAR Electronic Filing Instructions**

### **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://bsaeiling.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 SAR instructions and FinCEN guidance on use of special responses in 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>.

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 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 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 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 SAR version. FinCEN SAR items not on the prior 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 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. 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 CTR address format, record equivalent address information in the FinCEN CTR address items (except state) and ignore non-conforming data. The complete foreign address should be recorded in the 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 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 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 institution's customer are occurring on an ever-increasing basis. Since the implementation of the new FinCEN SAR in 2011, a significant number of SARs have been filed to record the events with the data being recorded in Part V, the 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 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 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 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 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 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 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 SAR based on the available information.

Bank D files a 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.**

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 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

**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 CTRs. Check box 1c "Continuing activity report" if the SAR continues reporting on previously-reported suspicious activity. If the 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 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 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 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:

- 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, 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 CTR 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)*  
a. *(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 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/MYY 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 "20. 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 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 if 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 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 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

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)

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)

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. STOLs, 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 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 BSAR 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)
  - 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
- 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 47. 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 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, a 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
- 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
  - h. 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 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 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

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.

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  
a. 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 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
- 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

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 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.

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.