UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

Frequently Asked Questions (FAQs)

Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs)

October 25, 2016

The Financial Crimes Enforcement Network (FinCEN) provides the following FAQs to supplement its advisory on cyber-events and cyber-enabled crime and assist financial institutions in reporting cyber-events and cyber-enabled crime through SARs.[1] The following FAQs supersede those published in 2001 regarding computer intrusion.[2] These new FAQs provide information and details not contained in the 2001 FAQs.

1. Q: What information should a financial institution include in SARs when reporting cyber-events and cyber-enabled crime?

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information.

While suspicious transactions may not always involve a cyber-event, relevant cyber-related information should still be included in SARs when available. For instance, financial institutions should include available Internet Protocol (IP) addresses and accompanying timestamps associated with fraudulent wire transfers being reported, even if a cyber-event was not involved in the suspicious activity.

Similarly, when suspicious transactions do involve cyber-events, a financial institution should include in SARs all relevant and available information regarding the suspicious transactions and the cyber-event—including the type, magnitude, and methodology of the cyber-event as well as signatures and facts on a network or system that indicate a cyber-event.

1. *See* FinCEN Advisory FIN-2016-A005 "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime" (October 2016).
2. These FAQs supersede "Frequently Asked Questions Regarding Computer Intrusion" published in the SAR Activity Review Trends, Tips, and Issues: Issue 3, Pages 39-41 (October 2001).

The following is a non-exhaustive list of relevant cyber-related information and identifiers associated with suspicious transactions and cyber-events that should be reported as available:

- Source and Destination Information:
  - IP address and port information with respective date timestamps in UTC
  - Uniform Resource Locator (URL) addresses
  - Attack vectors
  - Command-and-control nodes
- File Information:
  - Suspected malware filenames
  - MD5, SHA-1, or SHA-256 hash information
  - E-mail content
- Subject User Names:
  - E-mail addresses
  - Social media account/screen names
- System Modifications:
  - Registry Modifications
  - Indicators of Compromise (IOCs)
  - Common vulnerabilities and exposures (CVEs)[3]
- Involved Account Information:
  - Affected account information
  - Involved virtual currency accounts (case sensitive)

2. Q: How should a financial institution complete SARs when reporting cyber-events and cyber-enabled crime?

Financial institutions should follow FinCEN's existing guidance when submitting SARs related to cyber-events and cyber-enabled crime.[4] Financial institutions should include relevant information in pertinent SAR fields as well as a description of the facts surrounding the cyber-event or cyber-enabled crime in the narrative section. Recognizing that cyber-events and cyber-enabled crime may involve event-specific cyber-related information, FinCEN requests filing institutions to be consistent and use widely used and accepted terminology.[5]

Completing the SAR Form

Financial institutions should enter available cyber-related information and identifiers, identified in FAQ 1 above, in their designated SAR fields. For example, specific SAR fields are available for providing IP addresses (item 44), website/URL addresses (item 19a), and e-mail addresses (item 19). Relevant information with no pre-designated SAR field should be included in the SAR narrative.

3. Additional information on CVEs available at the National Vulnerability Database at https://nvd.nist.gov.
4. For further instructions on how to complete SARs, including information formatting, financial institutions should refer to the Frequently Asked Questions Regarding the FinCEN SAR (May 2013) and the latest FinCEN SAR Electronic Filing Instructions, both available at www.fincen.gov.
5. Financial institutions may use as a resource the Glossary of Key Information Security Terms (May 2013) and other publications issued by the National Institute of Standards and Technology (NIST), a non-regulatory federal agency within the U.S. Department of Commerce, available at http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Completing the SAR Narrative

Financial institutions should document and provide in the SAR narrative a detailed description of the suspicious activity (e.g., transactions, cyber-events) being reported. In addition, as described in FAQ 1, filers should include in the SAR narrative descriptive cyber-related information as well as cyber-related identifiers for which there is no pre-designated SAR field.

Filers may also include information as an attachment to the SAR. For example, filers may include in a SAR attachment patterns of online activity and other data, which may be easier to read and use in tabular format. FinCEN's SAR accepts a single comma separated value (CSV) file as an attachment. Please note that attachments are considered part of the SAR and are not a substitute for the narrative itself.

3. Q: How should cyber-events and cyber-enabled crime be characterized in SARs?

Financial institutions should categorize the activity being reported by selecting all applicable characterization checkboxes contained in Part II of the SAR, such as "Unauthorized Electronic Intrusion" (item 35q) or "Account Takeover" (item 35a). For SAR filing purposes, when suspicious activity (e.g., wire fraud) is also cyber-enabled crime, financial institutions should characterize the suspicious activity using the available SAR checkboxes (e.g. "Wire Fraud" item 31j). If no existing checkbox adequately characterizes the activity, filers should identify the suspicious activity in the "Other" field (item 35z) by entering widely-used and accepted terminology.[6] Filers can select more than one characterization checkbox.

4. Q: How does a financial institution report numerous cyber-events in SARs?

FinCEN recognizes that filing a SAR to report individual cyber-events may require significant time and resources and could detract from a financial institution's efforts to guard against more significant money laundering and cyber threats.

Accordingly, a financial institution may file a single *cumulative SAR* to report multiple cyber-events when they are too numerous to be reported individually and:

- are similar in nature and share common identifiers, such as those described in FAQ 1 above

or

- are believed to be related, connected, or part of a larger scheme.

6. See, NIST's Glossary of Key Information Security Terms (May 2013), available at http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Financial institutions can also use *cumulative SARs* to report mandatory and voluntary reporting of cyber-events.[7] Financial institutions should only use *cumulative SARs* when reporting cyber-events and not other types of suspicious activity, which must be reported following normal SAR filing procedures.

5. Q: Is a financial institution required to file SARs to report continuous scanning or probing of a financial institution's systems or network?

No. FinCEN recognizes that filing a SAR to report each time an institution's system or network is scanned or probed is impractical and could detract from a financial institution's efforts to guard against more significant money laundering and cyber threats. However, when filing a SAR on a reportable cyber-event, financial institutions may include information about the scanning and probing of their systems and networks if available and relevant. To the extent that a financial institution reports scanning and probing, it may do so using cumulative SARs when such activity is too numerous to be reported individually.

6. Q: Should a SAR be filed in instances where an otherwise reportable cyber-event is unsuccessful?

Yes. An otherwise reportable cyber-event should be reported regardless of whether it is considered unsuccessful. Rather, a financial institution is required to file a SAR to report any cyber-event if the institution knows, suspects, or has reason to suspect the cyber-event was intended to or could affect a transaction conducted or attempted by, at, or through the financial institution. See FinCEN's Advisory FIN-2016-A005 on Cyber-Events and Cyber-Enabled Crime.

7. Q: Does FinCEN now require financial institutions' BSA/AML units to have personnel/systems devoted to cybersecurity?

No. There are no new requirements or obligations for financial institutions. FinCEN's Advisory FIN-2016-A005 and these FAQs do not change existing BSA or other expectations or regulatory obligations. Financial institutions should continue to follow federal and state government agencies' and pertinent regulatory organizations' guidance and requirements on cyber-related reporting and compliance obligations. This guidance should not be interpreted in a manner inconsistent with guidance previously issued by FinCEN, U.S. government agencies, or other regulatory organizations.

7. FinCEN Advisory FIN-2016-A005 "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime" (October 2016) provides guidance on mandatory SAR reporting of cyber-events.

8. Q: Are BSA/AML personnel now required to be knowledgeable on cybersecurity and cyber-events?

No. There are no new requirements or obligations for financial institutions. A BSA/AML unit may work and collaborate as necessary with its institution's cybersecurity personnel, to assist in their ability to adequately identify and report suspicious activity, including cyber-events and cyber-enabled crime.

9. Q: Can financial institutions use Section 314(b) of the USA PATRIOT Act to share cyber-event and cyber-enabled crime information with other financial institutions?

Yes. Under Section 314(b), participating financial institutions may exchange information, including cyber-related information, regarding individuals, entities, organizations, and countries to identify and report money laundering and terrorist activities.[8] Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information voluntarily with one another—after notifying FinCEN and satisfying certain other requirements—under a safe harbor, which offers protections from liability under certain circumstances. In addition, under Section 314(b) any type of participating financial institution, such as a bank, may share information with any other participating institution, such as a credit card operator or a money transmitter.

Sharing cyber-related information and information related to cyber-event and cyber-enabled crime may:

- Aid in identifying and stopping cyber-events and cyber-enabled crime potentially connected to money laundering and terrorist activities.
- Build a more comprehensive and accurate picture of cyber-events and cyber-enabled crime potentially connected to money laundering or terrorist activities.
- Alert contacted financial institutions about customers whose information or credentials may have been compromised.
- Facilitate the filing of more comprehensive and complete SARs than would otherwise may have been filed, in the absence of 314(b) information sharing.

FinCEN's Section 314(b) Fact Sheet provides further information about the 314(b) information sharing program and outlines additional benefits available to program participants.[9]

8. Cyber-related information is information that describes technical details of activity and behavior, such as IP addresses, timestamps, indicators of compromise, and device identifiers. Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

9. Available at: https://www.fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf.