UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

FIN-2016-A005 **October 25, 2016**

Advisory

Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime

Cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats.

The proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system. The Financial Crimes Enforcement Network (FinCEN) issues this advisory to assist financial institutions in understanding their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

I. Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);

II. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;

III. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity; and

IV. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

This Advisory should be shared with:

- *Cybersecurity units*
- *Network administrators*
- *Risk departments*
- *Fraud prevention units*
- *BSA/AML management*
- *AML intelligence units*
- *AML analysts/investigators*

For the purpose of this advisory:[1]

Cyber-Event: An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.

Cyber-Enabled Crime: Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.

For the purpose of this advisory (continued):

Cyber-Related Information: Information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs). Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

Background

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions can play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs.

Value of BSA Reporting in Combating Cybercriminals and Cyber-Enabled Crime

FinCEN and law enforcement regularly use information financial institutions report under the BSA to initiate investigations, identify criminals, and disrupt and dismantle criminal networks. The cyber-related information that financial institutions include in this reporting is a valuable source of investigatory leads. Law enforcement has been able to use cyber-related information reported—such as IP addresses with timestamps, cyber-event data, and virtual-wallet information—to track criminals, identify victims, and trace illicit funds.

For example, BSA reporting by more than 20 financial institutions—on transactions related to cyber-enabled crimes—played an important role in the investigation of an internet-based company, its co-founders, and other collaborators. This company acted as an unregistered online money-transmitting business and offered digital currency services specifically designed to provide anonymity to facilitate international crime and money laundering. Criminals used this company to conduct over $6 billion in illicit transactions involving proceeds from cyber-attacks, credit card fraud, child pornography, Ponzi schemes, identity theft, and trafficking in narcotics and other contraband.

1. Unless otherwise defined by FinCEN, FinCEN uses the Glossary of Key Information Security Terms and other publications issued by the National Institute of Standards and Technology (NIST) for definitions of cyber-related terms. NIST is a non-regulatory federal agency within the U.S. Department of Commerce. Financial Institutions are encouraged to refer to the NIST Glossary for definitions.

Regulatory Expectations

This advisory does not change existing BSA requirements or other regulatory obligations for financial institutions.[2] Financial institutions should continue to follow federal and state requirements and guidance on cyber-related reporting and compliance obligations.[3]

Financial institutions should also note that filing a SAR does not relieve financial institutions from any other applicable requirements to timely notify appropriate regulatory agencies of events concerning critical systems and information or of disruptions in their ability to operate. In addition, the recently enacted Cybersecurity Act of 2015,[4] also known as the Cybersecurity Information Sharing Act (CISA), does not change any SAR-reporting requirements under the BSA,[5] SAR confidentiality rules,[6] or the safe harbor protections under section 314 of the USA PATRIOT Act.[7]

Guidance to U.S. Financial Institutions

The following guidance explains how BSA regulations and requirements apply to cyber-events, cyber-enabled crime, and cyber-related information.

I. SAR Reporting of Cyber-Events

Cyber-events targeting financial institutions often constitute criminal activity and can serve as means to commit a wide range of further criminal activity.[8] For instance, criminals may seek to obtain unauthorized electronic access to electronic systems, services, resources, or information to conduct unauthorized transactions. Cyber-events can target or affect funds

2. For previous guidance regarding cyber-related suspicious activity reporting, financial institutions may generally refer to: Suspicious Activity Report Instructions issued on June 2000, July 2003, and March 2011 (see in particular, instructions for when to make a report for unauthorized electronic intrusions a.k.a. computer intrusions); SAR Activity Review Trends, Tips, and Issues: Issue 3 (October 2001); FinCEN Advisory FIN-2011-A006 "Account Takeover Activity" (December 2011); and Frequently Asked Questions Regarding the FinCEN SAR (May 2013).
3. Financial institutions supervised by the federal banking agencies may also refer to additional guidance such as the Federal Financial Institutions Examination Council (FFIEC) Joint Statement on Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources (April 2014); FFIEC Joint Statements on Destructive Malware and Compromised Credentials (March 2015); FFIEC Joint Statement on Cyber Attacks Involving Extortion (November 2015); and the FFIEC IT Examination Handbook.
4. *See*, Pub. L. No. 114-113 and Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016). CISA authorizes, among other things, non-federal entities to share voluntarily specifically defined cyber-threat indicators and defensive measures for cybersecurity purposes.
5. *See*, 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20; as well as, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (June 2016).
6. *See*, 31 U.S.C. § 5318(g)(2).
7. *See*, 31 C.F.R. § 1010.540.
8. *See generally*, 18 U.S.C § 1030.

directly—such as in cases of fraud, identity/credential theft, and misappropriation of funds. Similarly, cyber-events can generate illicit proceeds—such as in cases of ransomware attacks and the sale of stolen proprietary information and credit card numbers.

Mandatory SAR reporting of cyber-events

A financial institution is required to report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets.[9] If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.

In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.[10]

Financial institutions should also be familiar with any other cyber-related SAR-filing obligations required by their functional regulator. For instance, the Office of the Comptroller of the Currency (OCC) requires national banks to file SARs to report unauthorized electronic intrusions.[11] The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) issued guidance concerning the filing of SARs to report certain computer-related crimes.[12]

9. *See*, 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000. 31 C.F.R. § 1022.320(a)(2).
10. Guidance on the reporting of Unauthorized Electronic Intrusions (UEIs) remains unchanged; see supra note 2. Financial institutions should report cyber-events as UEIs when such cyber-events meet the definition of a UEI. A UEI is defined as gaining access to a computer system of a financial institution to: a) remove, steal, procure or otherwise affect funds of the financial institution or the institution's customers; b) remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or c) damage, disable, disrupt, impair or otherwise affect critical systems of the financial institution.
11. *See*, OCC Bulletin OCC 2000-14 "Infrastructure Threats—Intrusion Risks" (May 2000).
12. *See*, FRB Supervisory Letter SR 97-28 "Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions" (November 1997); FDIC Financial Institution Letter FIL-124-97 "Guidance for Financial Institutions on Reporting Computer-Related Crimes" (December 1997); and NCUA Regulatory Alert 97-RA-12 "Guidance for Reporting Computer-Related Crimes" (December 1997).

The following examples illustrate situations in which SAR reporting of cyber-events is mandatory. These examples do not, however, describe all instances when cyber-events require the filing of a SAR.

Example 1: Through a malware intrusion (a type of cyber-event), cybercriminals gain access to a bank's systems and information. Following its detection, the bank determines the cyber-event put $500,000 of customer funds at risk, based on the systems and/or information targeted by the cyber-event. Accordingly, the bank reasonably suspects the intrusion was in part intended to enable the perpetrators to conduct unauthorized transactions using customers' funds.

The bank must file a SAR because it has reason to suspect the cybercriminals, through the malware-intrusion, intended to conduct or could have conducted unauthorized transactions aggregating or involving at least $5,000 in funds or assets. As explained in the next section, the bank should include all available information in the SAR relevant to the suspicious activity, including cyber-related information such as a description and signatures of the cyber-event, attack vectors, command-and-control nodes, etc.

Example 2: Through a cyber-event, cybercriminals gain access to a financial institution's systems/networks. The cyber-event exposes sensitive customer information such as account numbers, credit card numbers, balances, limits, scores, histories, online-banking credentials, passwords/PINs, challenge questions and answers, or other similar information useful or necessary to conduct, affect, or facilitate transactions.

By evaluating the cyber-event and the type of information sought by its perpetrators, the financial institution reasonably suspects the cyber-event may have targeted information for the purpose of conducting, facilitating, or affecting transactions aggregating to at least $5,000. For instance, the financial institution could reasonably suspect the cybercriminals intended to steal and sell the exposed sensitive customer information to other criminals for financial exploitation to include unauthorized transactions at the institution. As further described below, the targeted financial institution should file a SAR to report all relevant information, including cyber-related information and information pertaining to any related unauthorized transactions.

Examples 1 and 2 describe instances where a financial institution should file a SAR in response to a cyber-event. Although no actual transactions may have occurred in these examples, the circumstances of the cyber-events and the systems and information targeted could reasonably lead the financial institutions to suspect the events were intended to be part of an attempt to conduct, facilitate, or affect an unauthorized transaction or series of unauthorized transactions aggregating or involving at least $5,000 in funds or assets.

Example 3: A Money Services Business (MSB) knows or suspects a Distributed Denial of Service (DDoS) attack prevented or distracted its cybersecurity or other appropriate personnel from immediately detecting or stopping an unauthorized $2,000 wire transfer.

In this case, the financial institution should file a single SAR to report both the unauthorized wire transfer and the related DDoS attack. The financial institution should report the transaction because it was unauthorized and meets the filing threshold; and it should report the DDoS attack because the DDoS attack was perpetrated to conceal the unauthorized wire transfer.

Voluntary reporting of cyber-events

FinCEN encourages, but does not require, financial institutions to report egregious, significant, or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR.

To illustrate, consider a DDoS attack that disrupts a financial institution's website and disables the institution's online banking services for a significant period of time. After mitigating and investigating the DDoS attack, the affected financial institution determines the attack was not intended to and could not have affected any transactions. Although a financial institution is not required to report such DDoS attack, FinCEN encourages the financial institution to consider filing a SAR because the attack caused online banking disruptions that were particularly damaging to the institution. SAR reporting of cyber-events, even those that may not meet mandatory SAR-filing requirements, is highly valuable in law enforcement investigations.

II. Including Cyber-Related Information in SAR Reporting

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information. Because everyday financial transactions increasingly rely on electronic systems and resources, illicit financial activity often has a digital footprint, which may correspond to illicit actors and their associates, their activity, and related suspicious transactions.

Thus, financial institutions should include available cyber-related information when reporting *any* suspicious activity, including those related to cyber events as well as those related to other activity, such as fraudulent wire transfers. Cyber-related information includes, but is not limited to, IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information. FinCEN also encourages the filing of all such cyber-related information when a financial institution files a voluntary SAR. For additional information on reporting cyber-related information in SARs, please refer to these Frequently Asked Questions (FAQs) available on FinCEN's website.

Reporting cyber-related information involving cyber-events

When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR—in addition to any other related suspicious activity. As needed, financial institutions may also attach a comma separated value (CSV) file to SARs to report data, such as cyber-event data and transaction details, in tabular form.[13] For example, to the extent available, SARs involving cyber-events should include:

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

Financial institutions subject to large numbers of cyber-events may report them through a single cumulative SAR filing when such events are similar in nature. For instance, a financial institution may file one SAR to report several malware intrusions if these events share common characteristics and indicators such as the methodology used, the vulnerability exploited, and IP addresses involved.[14]

FinCEN also encourages financial institutions to incorporate cyber-related information into their BSA/AML monitoring efforts and report relevant cyber-related information in SARs. In the event a financial institution's filing software is not yet capable of including certain relevant information such as cyber-related information, as clarified by FinCEN in May 2013, the institution should manually complete discrete SAR filings until it updates its software to allow the inclusion such information.[15] Financial institutions can submit discrete SARs through FinCEN's BSA E-Filing System.

This advisory is not intended to, and does not, create any new obligation or expectation requiring financial institutions to collect cyber-related information as a matter of course.

13. A CSV file is a part of, but not a substitute for, the SAR narrative. In addition, like other information prepared in connection with a SAR filing but not attached to a SAR, an unattached CSV file is considered supporting documentation and should be accorded confidentiality to the extent it indicates the existence of a SAR.
14. See FAQs regarding the Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs (October 2016).
15. See Frequently Asked Questions Regarding the FinCEN SAR (May 2013).

III. Collaboration between BSA/AML and Cybersecurity Units

As the examples above illustrate, collaboration and ongoing communication among BSA/AML, cybersecurity, and other units will help financial institutions conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime. Accordingly, financial institutions are encouraged to internally share relevant information from across the organization including, as appropriate, with BSA/AML staff, cybersecurity personnel, fraud prevention teams, and other potentially affected units.

Information provided by cybersecurity units could reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units. For instance, BSA/AML units can use cyber-related information, such as patterns and timing of cyber-events and transaction instructions coded into malware among other things, to (1) help identify suspicious activity and criminal actors and (2) develop a more comprehensive understanding of their BSA/AML risk exposure. Likewise, cybersecurity personnel can use information provided by BSA/AML units to help the institution guard against cyber-events and cyber-enabled crime. In addition, this type of internal cooperation provides for more comprehensive and complete SAR reporting and is consistent with the principles involved in establishing a strong culture of compliance.[16]

IV. Sharing Cyber-Related Information between Financial Institutions

Financial institutions can work together to identify threats, vulnerabilities, and criminals. By sharing information with one another, financial institutions may gain a more comprehensive and accurate picture of possible threats, allowing for more precise decision making in risk mitigation strategies. FinCEN continues to encourage financial institutions to use all lawful means to guard against money laundering and terrorist activities presented through cyber-events and cyber-enabled crime.

To encourage information sharing, Section 314(b) of the USA PATRIOT Act extends a safe harbor from liability to financial institutions—after notifying FinCEN and satisfying certain other requirements—that voluntarily share information with one another for the purpose of identifying and, where appropriate, reporting potential money laundering or terrorist activities.[17] Under Section 314(b), financial institutions may share information, including cyber-related information, regarding individuals, entities, organizations, and countries for

16. *See*, FinCEN Advisory FIN-2014-A007 "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (October 2014).

17. For further information regarding Section 314(b), including requirements for sharing information, please refer to the Section 314(b) Fact Sheet available on FinCEN's website.

the purposes of identifying and reporting money laundering and terrorist activities. Thus, financial institutions may receive 314(b) safe harbor protections when sharing cyber-related information for the above mentioned purposes.[18]

Cyber-related information, such as information about specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses, for example, can help identify the individuals, entities, organizations, or countries involved or responsible for the cyber-event or cyber-enabled crime linked to money laundering or terrorist activities.

For Immediate Assistance, Contact Regulatory and Law Enforcement Agencies

Financial institutions needing immediate assistance in the event of a cyber-event or a cyber-enabled crime should contact appropriate regulatory and law enforcement agencies. Regulatory and law enforcement agencies can help affected financial institutions normalize systems and operations and, in some cases, reduce monetary losses. The U.S. Department of Homeland Security (DHS) published a fact sheet on obtaining threat and asset response assistance following a cyber incident.[19] In addition, the U.S. Department of Justice published a guide outlining appropriate government agencies to contact in the event of computer hacking, fraud, and other internet-related crime.[20]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov, (800) 767-2825 (Option 9), or (703) 905-3591 (Option 9). ***Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day)***. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

18. For information on sharing cyber-related information outside BSA safe harbor protections, please see the Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015.
19. The DHS fact sheet was issued pursuant to Presidential Policy Directive 41, which sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. The DHS fact sheet also lists key points of federal contact and is available at https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf.
20. Available at the Department of Justice website at http://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime.