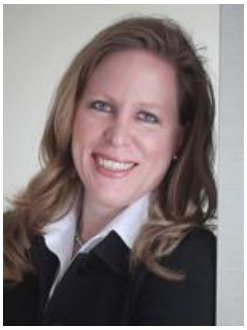
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FinCEN Cybercrime Advisory Expands SAR Requirements

By **attorneys with Crowell & Moring LLP**

Law360, New York (November 29, 2016, 2:01 PM EST) -- On Oct. 25, 2016, the U.S. Department of the Treasury's Financial Crimes Enforcement Network issued a new advisory to financial Institutions on cyber events and cyber-enabled crime as well as a related list of frequently asked questions.

Carlton Greene



Cari N. Stinebower

Evan D. Wolff

The advisory provides guidance to financial institutions on FinCEN's expectations with regard to: (1) reporting cyber-enabled crime and cyber events through suspicious activity reports (SARs); (2) including relevant and available cyber-related information (e.g., internet protocol addresses with time stamps, virtual-wallet information, device identifiers) in SARs; (3) collaboration within regulated institutions between Bank Secrecy Act/anti-money laundering units and in-house cybersecurity units to identify suspicious activity; and (4) sharing cyber-related information among financial institutions under existing safe harbor mechanisms used to identify and report potential terrorist activities and money laundering.

The advisory is characterized as interpretive guidance that does not change existing BSA requirements or impose additional regulatory obligations on financial institutions. However, some of the expectations in the guidance are likely to be new to most financial institutions, and have the potential to increase SAR reporting burdens substantially, both by expanding the types of events that must be reported as SARs and by expanding the types of information that must be gathered and included in all SARs.

The financial institutions affected by the advisory and the FAQs include not only banks but also casinos, money services businesses, broker-dealers, mutual funds, insurance companies offering particular types of insurance, futures commission merchants, introducing brokers in commodities, nonbank residential mortgage lenders or originators, and housing-related government-sponsored enterprises like Fannie Mae and Freddie Mac.

Definitions

FinCEN uses the following definitions in the advisory:

- ***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 or identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.

- ***Cyber-Related Information:*** Information that describes technical details of electronic activity and behavior, such as IP addresses, time stamps, indicators of compromise (IOCs), and device identifiers. Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

Mandatory Reporting of Cyber Events

Under the BSA, financial institutions must report any transaction conducted or attempted by, at, or through the institution that involves an aggregate of $5,000 or more in funds or other assets (or $2,000 for money services businesses) and which the institution knows, suspects or has reason to suspect: (1) involves funds derived from illegal activities or is intended or conducted to hide or disguise funds or assets derived from illegal activities 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; (2) is designed to evade any reporting or other requirements under the Bank Secrecy Act; (3) 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 bank knows of no reasonable explanation for the transaction after examining the available facts; or (4) involves the use of the institution to facilitate criminal activity. In addition to the required reporting above, a financial institution may file a SAR voluntarily on any "suspicious transaction that it believes is relevant to a potential violation of any law or regulation."

FinCEN's new advisory instructs that a financial institution should file a SAR if it "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." FinCEN recognizes that this standard may require the filing of SARs even in circumstances where no actual financial transactions ultimately occur or are attempted in connection with the cyber event. For purposes of determining whether the $5,000 threshold for reporting is triggered, the advisory instructs financial institutions to "consider in aggregate the funds and assets involved in or put at risk by the cyber-event." This includes, for example, the amount of funds present in accounts potentially affected by a cyber event, as well as amounts that may become available to cybercriminals as a result of data theft (e.g., credit card numbers).

The advisory provides specific examples of situations that require reporting under this standard, including a malware intrusion that a bank determines to have put $500,000 of customer funds at risk, as well as a cyber event that exposes sensitive customer information such as account numbers, credit card numbers and passwords that might be useful to conduct, affect or facilitate transactions aggregating to at least $5,000. In both examples, the advisory counsels that a financial institution must file a SAR, reasoning that although "no actual transactions may have occurred," the circumstances "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 transactions aggregating to at least $5,000 in funds or assets. In addition, the FAQs accompanying the advisory explain that reporting is required regardless of whether the cyber event at issue is considered to have been "successful," so long as there is reason to believe that the cyber event was intended to or could affect a transaction or series of transactions conducted or attempted by, at, or through the financial institution that exceed the reporting threshold. In the same vein, FinCEN provides a third example of mandatory reporting where a distributed denial of service (DDoS) attack on a money services business is reportable because it is determined to have been likely conducted as distraction to prevent cybersecurity or other personnel from detecting and stopping an unauthorized transaction through the institution.

Anticipating that many financial institutions may see large numbers of cyber events, FinCEN provides in the FAQs that financial institutions may report multiple cyber events in a single SAR when these are too numerous to be reported individually and (1) are similar in nature and share common identifiers; and (2) are believed to be related, connected, or part of a larger scheme. At the same time, the FAQs make clear that a financial institution is not required to file a SAR "each time an institution's system or network is scanned or probed," given that such reporting would be impractical and could detract from other efforts to guard against cyberthreats, though they note that financial institutions may include such information about the scanning and probing of their systems and networks when filing a SAR on an otherwise reportable cyber event.

According to the advisory and the FAQs, SARs relating to cyber events should include the following:

- Description and magnitude of the event
- Source and destination information, including:
- IP address and port information with respective date time stamps in UTC
  o Attack vectors
  o Command-and-control nodes
- File information, including:
- Suspected malware filenames
  o MD5, SHA-1, or SHA-256 hash
  o E-mail content
- Subject user names, including:

- E-mail addresses
  o Social media account/screen names
- System modifications, including:
- Registry modifications
  o Indicators of Compromise
  o Common vulnerabilities and exposures (CVEs)
- Involved account information, including:
- Affected account information
- Involved virtual currency accounts
- Known or suspected time, location, and characteristics or signatures of the event
- Other relevant IP addresses and their time stamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

The existing SAR reporting form already contains fields for some types of cyber-related information, such as IP addresses, website/URL addresses and e-mail addresses. FinCEN suggests that other cyber-related information should be put into the narrative fields of SARs, and also may be supplemented by attachments in a tabular format, for example in a comma separated value (CSV) file.

Separately, FinCEN notes that, even where reporting of a cyber event is not mandatory under BSA regulations, other laws may require reporting of these events, and financial institutions remain subject to any other such obligations. In particular, the federal banking agencies have their own requirements for the reporting of cyber events, and these are cross-referenced in the advisory.

Voluntary Reporting of Cyber Events

The advisory also encourages, though it does not require, financial institutions to report "egregious, significant, or damaging cyber-events and cyber-enabled crime" regardless of whether such events ordinarily would require the filing of a SAR. To illustrate, the advisory provides the example of a DDoS attack on a financial institution's website that results in a disruption of service for customers for a significant period of time but does not involve any related transactions or compromise of customer data. Although such an attack in isolation may not reasonably trigger SAR reporting requirements if no customer funds or assets were placed at risk, FinCEN notes that reporting of such cyber events is nevertheless "highly valuable in law enforcement investigations."

Including Cyber-Related Information in SARs

The advisory also explains FinCEN's expectation that financial institutions will include cyber-related information (including the data fields identified for cyber-event reporting above), whenever it is available, for any SAR, regardless of whether or not the SAR relates to a cyber event. This has the potential to substantially increase the amount of information that must be reported in the thousands of SARs that financial institutions now file on an annual basis, and seems likely to require compliance personnel to understand how to identify the availability and relevance of such information for inclusion in SAR reporting, or to have access to other financial institution personnel who will. FinCEN reasons that providing such information is part of a financial institution's obligation to provide complete and accurate reporting when filing a SAR.

Collaboration In-House Between BSA/Anti-Money Laundering Units and Cybersecurity Personnel

Accordingly, while the FAQs explain that a financial institution's BSA/AML personnel are not specifically required to be knowledgeable about cybersecurity and cyber events, FinCEN notes that collaboration with cybersecurity, anti-fraud and other knowledgeable personnel within a financial institution may assist AML compliance units in detecting cyber events and other suspicious activity that must be reported and in identifying relevant cyber-related information that must be included in SARs. FinCEN also specifically encourages financial institutions to incorporate cyber-related information into their AML monitoring efforts and to use cyber-related information to improve their AML risk assessments. Conversely, FinCEN suggests that cybersecurity personnel will be able to use information provided by BSA/AML units to improve their ability to guard against cyber events and cyber-related crime.

Sharing Cyber-Related Information Externally Among Financial Institutions

Finally, the advisory encourages financial institutions to make use of Section 314(b) of the USA Patriot Act and its implementing regulations, which allow financial institutions to register with FinCEN and then to share information with other registered institutions for the purpose of identifying and reporting activities that may involve money laundering or terrorist activity, as a means for increased sharing of cyber-related information. The advisory explains that information such as specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses "can help identify the individuals, entities, organizations, or countries involved or responsible for [a] cyber-event or cyber-enabled crime linked to money laundering or terrorist activities."

Practical Considerations

FinCEN's guidance is effective immediately. Banks and other affected financial institutions should begin now to consider what personnel, technology and methodology they will use to: (1) identify cyber events and assess when these require reporting under the new guidance, recognizing that, unlike traditional SARs, cyber events may require reporting even where no financial transaction is ever conducted, and even where an attempted intrusion is unsuccessful; (2) identify cyber-related information that must be

reported when filing any SAR, whether it relates to a cyber event or not; and (3) incorporate cyber-event and cyber-related information into AML risk assessments for the institution and into AML transaction monitoring and resolution. Given that many financial institutions experience thousands of attempts each day to improperly access their information, the first of these items may be especially resource-intensive. All of these likely will require close collaboration with and reliance on financial institution cybersecurity personnel, and perhaps new technology. Because most banks already are required to report intrusions and cybercrime by their prudential banking regulators, the burden of the new guidance will fall most heavily on nonbank financial institutions subject to SAR reporting requirements. Affected financial institutions also should be aware of the other cyber-reporting obligations they may have apart from those required under the BSA (some of which are mentioned in the advisory), and seek to take advantage of any efficiencies from combining reporting processes. Finally, although financial institutions should seek opportunities to make use of 314(b) to share cyber-related information, it is worth remembering, as FinCEN notes more than once, that the safe harbor for information sharing under the regulations implementing Section 314(b) is limited to the sharing of information for the purpose of identifying and reporting activities that may involve money laundering or terrorist activity. Similarly, the financial institution that receives the information may use it only for such purposes.

Carlton Greene is a partner in the Washington, D.C., office of Crowell & Moring LLP and a former chief counsel at FinCEN.

Cari N. Stinebower, another Washington-based partner, is a former counsel for the U.S. Department of the Treasury's Office of Foreign Assets Control.

Evan D. Wolff is also a partner in Crowell & Moring's Washington office. He has served as an adviser at the Department of Homeland Security and other government agencies and was involved in the development of the DHS..

James (J.J.) Saulino, Adeoye O. Johnson and Matthew B. Welling are associates in the firm's Washington office.