WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Increased Financial Regulatory Focus for Enhanced Reporting of Cyber-Events and Cyber-Enabled Crime

November 3, 2016

AUTHORS

Elizabeth P. Gray | James E. Anderson | James R. Burns | Daniel K. Alvarez | Katherine Doty Hanniford

Financial regulators at the federal and state levels are showing greater interest in enhancing reporting obligations arising from cyber-events and cyber-enabled crime.[1] Two recent actions highlight this trend: On October 25, 2016, FinCEN issued an Advisory[2] and related Frequently Asked Questions ("FAQs")[3] regarding financial institutions' reporting obligations in connection with cyber-events and cyber-enabled crime. Meanwhile, the New York Department of Financial Services (the "NYDFS") has proposed sweeping compliance and reporting regulations that will be implemented as modified after a 45-day notice and comment period closes on November 11, 2016.

The FinCEN Advisory applies to financial institutions, which FinCEN defines as any individual or entity doing business in one or more of the following capacities: bank (except bank credit card systems); broker or dealer in securities; money services business; telegraph company; casino; card club; or person subject to supervision by any state or federal bank

1 *See, e.g.*, "SEC Proposes Rule Requiring Investment Advisers to Adopt Business Continuity and Transition Plans," July 26, 2016, *available* here.

2 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, FIN-2016-A005, October 25, 2016, *available* here.

3 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, *available* here.

supervisory authority. The NYDFS regulations affect entities supervised by the NYDFS under banking law, insurance law, and financial services law. Its regulations would apply to covered entities, which include major banks, insurance companies, mortgage brokers, credit unions, holding companies, and investment companies, as well as smaller entities.

FinCEN Advisory — Obligations and Encouragement to Report Cyber-Events

The FinCEN Advisory states that financial institutions should file Suspicious Activity Reports ("SARs") in the event of an attempted or actual cyber-event or cyber-enabled crime, and outlines guidance for mandatory and voluntary reporting, the inclusion of cyber information in other SARs reporting, and information sharing to assist in combating cyber threats across the banking and financial sector. The Advisory repeatedly stressed the value to law enforcement of SARs reporting on cyber activity.

The Advisory and FAQs follow another recent Advisory warning financial institutions of email compromise fraud schemes, in which criminals hack into and gain control of bank customer, bank executive, or third-party service provider email accounts in order to conduct fraudulent wire transfers, and outlining the content of appropriate SARs reporting. That Advisory also offered law enforcement assistance to victims.[4]

Mandatory reporting

A financial institution must report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates $5,000 or more in funds or other assets.[5] Under the new guidance, if a financial institution knows, suspects, or has reason to suspect that an attempted cyber-event or cyber-enabled crime—irrespective of whether the attempt was successful—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 and is subject to mandatory SAR reporting. To reiterate, even in instances where no actual transactions may have occurred, the circumstances of cyber-events and the systems and information put at risk could lead a financial institution to rightly suspect that the events were intended to be part of an attempt to conduct, facilitate, or affect an unauthorized transaction or series of transactions. Under such circumstances, the institution must file a SAR. FinCEN views such attempts as reportable because they are unauthorized, relevant to a possible legal or regulatory violation, and routinely involve efforts to acquire funds through illegal activities.

The guidance suggests that financial institutions consider all available information surrounding the cyber-event, including its nature and the information and systems targeted, in determining whether a cyber-event should be reported. Financial institutions should consider the aggregate amount of funds or assets involved or put at risk by the cyber-event. As a

[4] Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes, FIN-2016-A003, September 6, 2016, *available* here.

[5] *See* 31 C.F.R. §§ 1020.320, 1021.320, 1022.302, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20.

practical matter, therefore, it is likely that even small or relatively limited attempted cyber-events would be considered eligible for mandatory reporting.

Voluntary reporting

FinCEN does not require financial institutions to report cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR. However, FinCEN encourages financial institutions to report "egregious, significant, or damaging" cyber-events or cyber-enabled crime. As an example, FinCEN encourages the reporting of a distributed denial of service ("DDoS") attack that is disruptive but later determined not to have been intended to affect transactions. Nevertheless, the damage of the disruption to the institution, as well as the valuable law enforcement information that could be gained, weigh in favor of voluntarily reporting the cyber-attack.

Inclusion of cyber information in SARs reporting

FinCEN views the inclusion of cyber-related information as integral to filing a complete and accurate SAR. A financial institution should include all relevant and available information regarding the suspicious transactions and cyber-event, including the type, magnitude, and methodology of the cyber-event as well as the signatures and facts that indicate a cyber-event. To the extent available, SARs involving cyber-events should include:

- Description and magnitude of the event
- Methodologies used
- Subject user names
- Source and destination information
  - IP addresses, port information with timestamps in UTC
  - Uniform Resource Locator (URL) addresses
  - Attack vectors
  - Command and control nodes
- Involved account information
  - Affected account information
  - Involved virtual currency accounts
- Known or suspected time, location, and characteristics of the event
- Device identifiers
- System modifications
  - Registry modifications
  - Indicators of compromise
  - Common vulnerabilities and exposures (CVEs)
- File information
  - Suspected malware filenames
  - MD5, SHA-1, SHA-256 hash information
  - E-mail content
- Any other relevant information

In instances where certain cyber-events may be too numerous to be reported individually and the cyber-events are either similar in nature and share common identifiers, as listed above, or are believed to be related, connected, or part of a larger scheme, a financial institution may file a single, cumulative SAR. The cumulative SAR may be used for mandatory or voluntary reports but may be used only for cyber-events, not other suspicious activities.

Information sharing

The advisory encourages financial institutions to share information in two ways: (i) internally among key stakeholders; and (ii) externally with other financial institutions via Section 314(b) of the USA PATRIOT Act. Both lines of information sharing would promote a more comprehensive threat assessment and sharpen risk management strategies regarding cyber events and cyber-enabled crime. In this advisory, FinCEN encourages financial institutions to coordinate internally across departments, including BSA/AML staff, cybersecurity personnel, fraud prevention teams, and other units as appropriate, in order to bolster a financial institution's pattern recognition and response capabilities. FinCEN views this coordination as consistent with its previous guidance regarding a strong culture of compliance.[6]

The advisory also encourages financial institutions to work together under Section 314(b) of the USA PATRIOT Act, which provides a safe harbor for participating institutions. While the safe harbor requires institutions to notify FinCEN and satisfy certain other requirements, information sharing may benefit financial institutions by (i) providing information that assists an institution in identifying and mitigating cyber-events and cyber-related crime; (ii) providing an avenue to alert other institutions about customers whose information or credentials may have been compromised; and (iii) facilitating a more comprehensive understanding of cyber-events or cyber-enabled crime, which could also lead to better SARs and additional useful information for law enforcement purposes.

Other reporting considerations

The guidance reiterates that filing a SAR does not exempt financial institutions from other applicable reporting requirements, such as those triggered by events concerning critical systems and information or of disruptions in their operations.

New York Department of Financial Services' Proposed Regulations

We further note that in addition to the existing reporting requirements, the NYDFS's proposed regulations contemplate an aggressive compliance and reporting regime.[7] The proposed regulations would require the designation by an institution of a "qualified individual" to serve as Chief Information Security Officer, responsible for overseeing and implementing its cybersecurity program and policy. The regulations include technological requirements such as limiting access privileges,

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

7 23 NYCRR § 500.0 (2016).

requiring encryption and multi-factor authentication, and certain provisions regarding information security would also extend to third-party service providers. Covered entities would be expected to conduct penetration testing annually and vulnerability assessments quarterly. There are also significant recordkeeping requirements, most notably the implementation of an audit trail sufficient to reconstruct all financial transactions, accounting, and data logging necessary to respond to a cyber-event or cyber-enabled crime, all of which must be maintained for six years.

The reporting requirement is among the more stringent provisions of the proposed regulations, and is more aggressive than every other state data-incident reporting requirement currently in place in the United States. The proposed reporting regime would be automatically triggered by any notice made by a covered entity to a government or self-regulatory agency, or any potential tampering with or access to non-public information. The institution would have 72 hours to report such a notice, potential tampering, or access to the NYDFS. In addition, the proposed regulations would require financial institutions to file a report within 72 hours upon the occurrence of a cyber-event that is reasonably likely to materially affect normal operations or that affects non-public information. Financial institutions would also need to file a report within 72 hours of identifying any material risk of imminent harm relating to its cybersecurity program.

Conclusion

While the FinCEN Advisory does not require a financial institution to hire additional personnel, it does strongly encourage enhanced coordination at the institution level and additional reporting and information sharing outside of the institution. Thus, institutions should consider how to allocate responsibility for internal coordination and reporting purposes among affected business units. Those institutions that will also become subject to the NYDFS regulations upon their implementation should consider whether existing resources are sufficient to cover the enhanced compliance, technological, recordkeeping, and reporting requirements currently contemplated by the regulations.

The FinCEN Advisory suggests a holistic approach to assessing whether a cyber-event should be reported, and in underscoring that attempted cyber-events are eligible for reporting, the Advisory recommends that an institution aggregate the funds or assets potentially put at risk by such an attempt. Coupled with its recommendation to voluntarily report cyber-events or cyber-enabled crime that otherwise would not merit the filing of a SAR, the Advisory's guidance represents a broadening of the scope of SARs reporting and corresponding information sharing opportunities.

Nevertheless, there may be additional consequences of filing voluntary SARs, as regulators continue to adapt to the emerging cyber threat. For example, should the NYDFS regulations be finalized in their current form, it appears that filing a voluntary SAR would trigger NYDFS reporting obligations. Recent FinCEN Advisories note the benefits to law enforcement and victim assistance that SARs reporting facilitates. In the face of near constant cyber-events and cyber-enabled crime, entities should weigh the advantages of information sharing against what in the past would have been viewed as reputational risk for voluntary reporting.

If you have any questions regarding this memorandum, please contact Elizabeth P. Gray (202-303-1207; egray@willkie.com), James E. Anderson (202-303-1114; janderson@willkie.com), James R. Burns (202-303-1241; jburns@willkie.com), Daniel K. Alvarez (202-303-1125; dalvarez@willkie.com), Katherine Doty Hanniford (202-303-1157; khanniford@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

November 3, 2016