Cullen | Dykman

FinCEN Issues Advisory and FAQs Regarding Reporting Cyber-Events

October 27, 2016

The Financial Crimes Enforcement Network ("FinCEN") has issued an advisory ("Advisory") and Frequently Asked Questions ("FAQs") to assist financial institutions in reporting cyber-events, cyber-enabled crime, and cyber-related information through Suspicious Activity Reports ("SARs"). The Advisory and FAQs, however, do not change existing Bank Secrecy Act ("BSA") requirements or other regulatory obligations for financial institutions, which are expected to continue to follow federal and state requirements and guidance on cyber-related reporting and compliance obligations.

The Advisory is intended to help financial institutions understand their BSA obligations regarding cyber-events and cyber-enabled crime,[1] and the FAQs supplement the Advisory by discussing certain anticipated issues. In the Advisory, FinCEN instructs financial institutions on: (1) reporting cyber-enabled crime and cyber-events through SARs; (2) including relevant and available cyber-related information in SARs; (3) collaborating between BSA/Anti-Money Laundering ("AML") units and in-house cybersecurity units to identify suspicious activity; and (4) sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorist financing, and cyber-enabled crime.

SAR Reporting of Cyber-Events

Generally, 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. 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. Thus, cyber-events targeting financial institutions that could affect a transaction or series of transactions over the reporting threshold amount would be reportable as suspicious transactions.

The FAQs point out that an otherwise reportable cyber-event should be reported regardless of whether it is considered unsuccessful. FinCEN also 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.

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. The Advisory provides some examples of situations in which SAR reporting of cyber-events is mandatory. Financial institutions should also be familiar with any other cyber-related SAR filing obligations required by their functional regulator.

In light of the continuous scanning and probing of financial institutions' systems and networks, the FAQs point out that filing a SAR to report each scanning or probing event is impractical and could detract from an institution's efforts to guard against more significant threats. The FAQs clarify that institutions are not required to file SARs to report such events.

The FAQs also make clear that a financial institution is allowed to file a single cumulative SAR to report multiple cyber-events when they are too numerous to be reported individually and are either: (i) similar in nature and share common identifiers or (ii) believed to be related, connected, or part of a larger scheme.

Including Cyber-Related Information in SAR Reporting

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available and should follow FinCEN's existing guidance when submitting SARs related to cyber-events and cyber-enabled crime. 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.

Financial institutions should be sure to include any and all 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. For example, to the extent available, SARs involving cyber-events should include: (i) description and magnitude of the event; (ii) known or suspected time, location, and characteristics or signatures of the event; (iii) indicators of compromise; (iv) relevant IP addresses and their timestamps; (v) device identifiers; (vi) methodologies used; and (vii) other information the institution believes is relevant.

Collaboration Between BSA/AML and Cybersecurity Units

The Advisory emphasizes the importance of collaboration and ongoing communication among BSA/AML, cybersecurity, and other units in order to 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. FinCEN, however, is not imposing any new requirements or obligations for financial institutions, such as requiring a financial institution's BSA/AML unit to have personal and/or systems devoted to cybersecurity or requiring BSA/AML personnel to be knowledgeable on cybersecurity (i.e., a BSA/AML unit may work and collaborate as necessary with its institution's cybersecurity

personnel).

Sharing Cyber-Related Information Between Financial Institutions

The Advisory stresses the importance of financial institutions working together to identify threats, vulnerabilities, and criminals, and highlights Section 314(b) of the USA PATRIOT Act. Section 314(b) provides a safe harbor from liability for financial institutions that share cyber-related information with other institutions for the purposes of identifying and, where appropriate, reporting potential money laundering or terrorist activities. To attain this protection, institutions must notify FinCEN and satisfy certain other requirements.

Further Information

The Advisory may be found here and the FAQs may be found here. In addition to submitting SAR reports, financial institutions must continue to adhere to federal and state laws, regulations, and guidance with respect to reporting cybersecurity incidents. For instance, New York State General Business Law section 899-aa requires a business to report a security breach to affected individuals and, in the event that any New York residents are to be notified, obligates the business to notify certain state agencies as to the timing, content and distribution of the customer notices, and approximate number of affected persons. Additionally, according to the 2005 GLBA Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, a financial institution should also notify its federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive consumer information. Our advisory regarding the new cybersecurity regulation proposed by the New York State Department of Financial Services may be found here.

If you have any questions regarding the Advisory, the FAQs, or cybersecurity procedures in general, please feel free to contact Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com, Kevin Patterson at 516-296-9196 or via email at kpatterson@cullenanddykman.com, or Adam Barazani at 516-357-3767 or via email at abarazani@cullenanddykman.com.

Practices

- Banking and Financial Services
- Regulatory and Compliance

Industries

- Financial Institutions

Attorneys

- Kevin Patterson

- Joseph D. Simon