HUNTON& WILLIAMS

Client Alert

November 2016

FinCEN Issues Advisory on SAR Reporting Obligations Involving Cyber Crime; Interprets Regs Broadly to Require Reporting of Cyber Events Intended or Having Potential to Affect Transactions

On October 25, 2016, the United States Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Advisory to help financial institutions understand how to fulfill their Bank Secrecy Act (BSA) obligations with regard to cyber-events and cyber-enabled crime.[i] The advisory indicates that SAR reporting is mandatory for cyber-events where the financial institution "knows, suspects or has reason to suspect a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions…." Implementing this new guidance will require increased collaboration between AML and cybersecurity or IT departments in large institutions, and may create challenges for smaller banks that are more likely to outsource their cybersecurity functions.

Reporting Cyber-Enabled Crime and Cyber-Events

In addition to maintaining cyber-related SAR-filing obligations stipulated by their functional regulator, financial institutions are mandated to report suspicious "cyber-events" or "cyber-enabled crime" involving or aggregating $5,000 or more in funds or other assets and conducted or attempted by, at or through the institutions. The key terms are defined as follows:

- ***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.[ii]

Illustrative examples provided in the Advisory indicate that the value of a cyber-event to be noted in the SAR (and used to trigger the $5,000 threshold) is the amount of customer funds at risk based on the information targeted by the intrusion. Banks are also encouraged to voluntarily report "egregious, significant, or damaging cyber-events and cyber-enabled crime" that may not require the filing of an SAR, such as an attack that disables an institution's online banking services for a significant period but does not pose any risk to transactions. FinCEN states that such SAR reporting is highly valuable to law enforcement investigations even though the intelligence does not relate to specific transactions.

Financial institutions are advised to file complete and accurate reports that include available cyber-related information, such as IP addresses with timestamps, virtual-wallet information, device identifiers and cyber-event information when reporting *any* suspicious activity. FinCEN notes that, provided the events are similar in nature, financial institutions subject to large numbers of cyber-events can report them under a single cumulative SAR filing. It also encourages financial institutions to incorporate cyber-related information into their BSA/AML monitoring efforts.

Increased Internal and External Information Sharing

FinCEN advises financial institutions to share relevant information internally, including, as appropriate, among BSA/AML staff, cybersecurity personnel, fraud prevention teams and other potentially affected units, to improve the quality of SAR reporting and create a strong culture of compliance. This underscores FinCEN's prior warnings to institutions against "communication silos" as outlined in the 2014 FinCEN Advisory on promoting a culture of compliance.[iii] The current advisory notes that the failure to properly communicate and share information between an institution's AML group and cybersecurity team may form the basis of an enforcement action.

FinCEN also encourages financial institutions to use all lawful means to guard against money laundering and terrorist activities presented through cyber-events and cyber-enabled crime by communicating with other financial institutions, and suggests that such information sharing could improve the institutions' risk mitigation strategies. The Advisory notes that the safe harbor from liability afforded to financial institutions under the Patriot Act encompasses Section 314(b), which allows financial institutions to "share information, including cyber-related information regarding individuals, entities, organizations, and countries for the purposes of identifying and reporting money laundering and terrorist activities." FinCEN has previously stated its perception that Section 314(b) exchanges have been underutilized by the industry and is encouraging the industry to increase information sharing under the statute as part of its AML compliance program.

While FinCEN notes that its latest advisory "does not change existing BSA requirements or other regulatory obligations for financial institutions," it is clear that FinCEN believes that the industry should be doing more to monitor and report potentially suspicious cyber-related activities. The notion that any intrusion that has the *potential* to impact financial transactions in excess of $5,000 requires an SAR filing is a broad interpretation of what constitutes an attempt to conduct a transaction. Historically, FinCEN regulatory guidance has focused more on actual, rather than attempted, cyber-intrusions,[iv] and there is little regulatory guidance generally as to what constitutes an attempt for purposes of SAR reporting requirements. The takeaway here is that, at least in the context of cyber-events and cyber-enabled crime, the potential alone to affect a transaction(s) in excess of $5,000 may be enough to trigger an SAR.

In reviewing the new guidance, institutions should consider (1) whether their AML risk assessment reflects the institution's history of, and potential exposure to, cyber-related activities; (2) whether their AML policies and procedures provide sufficient guidance to enable staff to detect and report cyber-related activities; (3) whether the institution's cyber-related monitoring system is commensurate with the institution's cyber risk profile; (4) whether there is a process by which employees with AML oversight communicate with in-house or outside cybersecurity resources to share information; and (5) whether cyber-related metrics and activities are monitored by audit (or independent risk management) and reported to senior management and the board of directors. Notwithstanding FinCEN's position that the new guidance does not impose any new requirements or obligations, financial institutions should take steps to incorporate the guidance in existing compliance procedures and be able to document any changes made for regulators.

Contacts

Laura Colombell Marshall
lmarshall@hunton.com

Peter G. Weinstock
pweinstock@hunton.com

Amy Sims Bowen
abowen@hunton.com

Shaswat (Shas) K. Das
sdas@hunton.com

[i] FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime" (October 25, 2016).

[ii] *Id.* (citing "Glossary of Key Information Security Terms" published by National Institute of Standards and Technology).

[iii] FIN-2014-A007, "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (August 11, 2014).

[iv] *See*, e.g., SAR Activity Review, Trends Tips & Issues (Oct. 2001) (discussing observed trends in SARs for computer intrusion, defined as actually gaining access to a financial institution's computer system for illicit purposes); FIN-2011-A016, *Account Takeover Activity* (Dec. 19, 2011) (providing guidance on filing SARs in connection with suspicious activity on a customer's account taken over by an unauthorized party).