CLIFFORD
CHANCE

Client briefing November 2016

AML and Cybersecurity: FinCEN's Advisory

On October 25, 2016, the Financial Crimes Enforcement Network ("**FinCEN**") issued an advisory providing guidance to financial institutions on how Bank Secrecy Act ("**BSA**") regulations apply to cyber events, cyber-enabled crime, and cyber-related information. In particular, the advisory focuses on Suspicious Activity Reports ("**SARs**") submissions for both cyber-events and cyber-related information. The advisory provides guidance with respect to: (i) SAR reporting in connection with cyber-enabled crime and cyber events; (ii) including relevant cyber-related information in SARs; (iii) encouraging collaboration between in-house cybersecurity units and AML units; and (iv) sharing cyber-related information among financial institutions to combat money laundering, terrorism financing, and cyber-enabled crime. The advisory provides SAR-filing related guidance in the context of cyber events. FinCEN states specifically that the advisory "does not change existing BSA requirements or other regulatory obligations for financial institutions."

Definitions

The advisory notes that unless defined, FinCEN uses the Glossary of Key Information Security Terms and other publications issued by the National Institute of Standards and Technology ("**NIST**") for cyber-related terms. In providing this guidance, FinCEN notes the definitions of the following terms:

- **Cyber-Event**: An **attempt** to compromise or gain unauthorized electronic access to electronic systems, services, resources or information (emphasis added).
- **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.
- **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.

Mandatory and Voluntary Reporting of Cyber Events

FinCEN provides guidance on mandatory and voluntary reporting, delineating trigger requirements for SARs as well as a description of the information that FinCEN would like to have but does not otherwise require by law.

The advisory reviews the regulatory requirements for submitting a SAR – suspicious transactions in the aggregate of $5,000[1] or more – and then explains how a cyber-event might be considered. Regardless of success, the advisory states, any cyber-event intended "in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions" should be considered an attempted suspicious transaction. An unauthorized transaction does not have to be successful to trigger the SAR requirement. FinCEN stresses that mere attempt is the threshold of consideration because it is "unauthorized [and] relevant to a possible violation of law or regulation," and cyber-events "regularly involve efforts to acquire funds through illegal activity."

The advisory uses various examples of required reporting to emphasize that the determination to report is a holistic process. Included in the open-ended consideration factors are: the nature of the cyber-event, the information and systems targeted, and the aggregate funds and assets implicated or put at risk. The three examples demonstrate mandatory reporting in: 1) a malware intrusion that placed $500,000 in customer funds at risk and that could have conducted unauthorized transactions, 2) a cyber-event exposing sensitive customer information, which could then be sold or used for further financial exploitation aggregating to over $5,000, and 3) an MSB suffering a Denial of Service Attack, which may have been used to conceal an unauthorized $2,000 wire transfer. The second example is particularly noteworthy because it might apply to a broad range of cyber-events, even unsuccessful ones.

Finally, FinCEN encourages voluntary SAR reporting for "egregious, significant, or damaging cyber-events and cyber-enabled crime."

Including Cyber-Related Information in SAR Reporting

As part of a financial institution's duty to file complete and accurate SARs, the advisory notes that *any* SAR, even one unrelated to a cyber event (such as a fraudulent wire transfer), should include all available cyber-related information. This information could include: IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information. Furthermore, FinCEN recommends that financial institutions incorporate cyber-related information into their BSA/AML monitoring efforts.

Collaboration between BSA/AML and Cybersecurity Units

The advisory also encourages financial institutions to share this information internally to foster collaboration between BSA/AML staff, cybersecurity personnel, fraud and prevention teams, and any other business units. Internal cross-cooperation will build synergy and is consistent with compliance culture.

Sharing Cyber-Related Information between Financial Institutions

---

[1] FinCEN notes that the monetary threshold for Money Services Businesses ("**MSBs**") SARs is set at $2,000, and one of the examples makes note of this.

In addition to sharing cyber-related information internally, FinCEN recommends that financial institutions should share this information with each other to gain a more comprehensive and accurate picture of possible threats. This will allow more precise decision-making for risk mitigation strategies. The advisory notes that firms may take advantage of the information sharing safe harbor benefits provided by Section 314(b) of the PATRIOT Act.

Conclusion

While FinCEN's advisory does not change pre-existing requirements, it provides guidance concerning FinCEN's expectations on SAR reporting of cyber-events and cyber-related information. Such expectations will by their nature require financial institutions AML/BSA units to work closely with their cybersecurity units. Notably FinCEN will expect SAR filing for cyber events and unauthorized transactions that are only attempted. The advisory underscores that financial institutions should use a holistic decision-making process to assess whether a SAR should be made. Financial institutions should be mindful of FinCEN's SAR filing expectations and should implement procedures designed to ensure that SARs are appropriately filed in connection with cyber events.

Authors

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon
@cliffordchance.com

Daniel Silver
Partner
T: +1 212 878 4919
E: daniel.silver
@cliffordchance.com

Philip Angeloff
Counsel
T: +1 202 912 5111
E: philip.angeloff
@cliffordchance.com