FINCEN LOOKS TO FINANCIAL INSTITUTIONS TO FILE SARS REGARDING CYBER-EVENTS

Date: 4 November 2016

Cyber Law and Cybersecurity Alert

By: Mark A. Rush, Stanley V. Ragalevsky, Rebecca H. Laird

On October 25, 2016, the Financial Crimes Enforcement Network ("FinCEN") issued an advisory (the "Advisory") explaining the obligations a "financial institution"[1] might have under the Bank Secrecy Act ("BSA") regarding "cyber-events and cyber-enabled crime."[2] The Advisory states that even if an actual financial transaction did not take place as result of a cyber-event, a financial institution may still be required to file a Suspicious Activity Report ("SAR") in certain circumstances. Because of this, a covered financial institution should reconsider its obligations under the BSA after a cyber-event.

BACKGROUND

The BSA is a complex set of federal laws and regulations that require financial institutions to maintain records, make reports (including SARs), and conduct due diligence as a means of helping the federal government detect financial crimes. SARs provided to FinCEN are confidential and not discoverable in civil litigation.[3] FinCEN, a bureau within the Treasury Department, is tasked with enforcing the BSA. While advisories, like the one FinCEN issued on October 25, 2016, do not have the force of law, they represent FinCEN's current interpretation of the law on which FinCEN can be expected to rely in investigations. Failure to comply with BSA requirements can have costly consequences.

MANDATORY SAR REPORTING OF CYBER-EVENTS

The Advisory states that 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." It explains that when a financial institution knows or reasonably suspects that a cyber-event was intended to facilitate a transaction, it should be considered "part of an attempt to conduct a suspicious transaction." This means that even if the cyber-event was unsuccessful (i.e., no money was actually transferred or no other assets were stolen), it could still be enough to warrant a SAR filing. FinCEN provided an example to demonstrate this point:

> *Through a malware intrusion (a type of cyber-event), cybercriminals gain access to a bank's systems and information. Following its detection, the bank determines the cyber-event put $500,000 of customer funds at risk, based on the systems and/or information targeted by the cyber-event. Accordingly, the bank reasonably suspects the intrusion was in part intended to enable the perpetrators to conduct unauthorized*

©2005-2026 K&L Gates LLP. All Rights Reserved.

> *transactions using customers' funds.*

FinCEN states that under these circumstances, the financial institution must file a SAR, even though no actual transaction may have occurred.

Under this broad mandate, financial institutions should consider the possibility of filing a SAR after any cyber-event, even if the primary objective of the cyber-event does not appear to be theft of money. FinCEN points out that account numbers, scores, passwords, and PINs all have value and count towards the $5,000 threshold because the stolen information could lead to later unauthorized transactions. Even attacks like a Distributed Denial of Service ("DDoS") could lead to a SAR filing. A DDoS occurs when a cybercriminal interrupts a company's web services by flooding the company's server with requests. Sometimes the intentions of a cybercriminal using a DDoS attack are difficult to discern. Cybercriminals may initiate DDoS attacks for extortion, hacktivism, or simply to cause mischief. FinCEN points out that DDoS attacks can be used as a smokescreen for other less obvious attacks that could put more than $5,000 at risk. In those cases, according to FinCEN, a SAR should be filed.

CYBER-RELATED INFORMATION IN A SAR FILING

FinCEN requires that a financial institution "file complete and accurate reports that incorporate all relevant information available, including cyber-related information." It specifically requests that financial institutions include IP addresses with timestamps, virtual-wallet information, and device identifiers. Some financial institutions may not have access to the sophisticated technology required to collect this cyber-event information. If they do, FinCEN requires that this information, along with any other information, such as fraudulent transfers related to the cyber-event, be reported in the SAR.

COLLABORATION BETWEEN BSA/AML AND CYBERSECURITY UNITS

In the Advisory, FinCEN requests the various departments tasked with security within a financial institution to collaborate and develop a comprehensive approach to security. FinCEN states that information provided by "cybersecurity units could reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units" and could lead to a better understanding of the risk exposure in the wake of a cyber-event.

FinCEN encourages, but does not require, the sharing of information among financial institutions as a way to gain a more accurate picture of possible threats. Further, it does not mandate that financial institutions share information by any particular method. If a financial institution is interested in this approach, there are third-party originations that can facilitate information and collaboration, such as the National Cyber-Forensics & Training Alliance ("NCFTA"). The NCFTA is a nonprofit entity that defends against cyber-based threats by bringing public, private, and academic sectors together in one space to share information and resources as a united front against cyber threats.[4]

CONCLUSION

©2005-2026 K&L Gates LLP. All Rights Reserved.

Although FinCEN has previously addressed SAR filings in the wake of a cyber-event, its most recent statement that SAR filings are mandatory in some circumstances signals that FinCEN will apply an aggressive approach to civil enforcement in the cybersecurity space. Financial institutions that experience a cyber-event should consider how the BSA, or other federal laws,[5] might apply to them to avoid enforcement or to build a robust compliance plan.

Notes:

[1] The Bank Secrecy Act broadly defines the phrase "financial institution." It includes much more than just banks. For example, institutions like a broker dealer, a currency exchange, an insurance company, a pawn broker, a travel agency, a car dealer, a money transmitter, or a casino each explicitly fall under the definition of "financial institution." 31 U.S.C. § 5312(a)(2).

[2] Financial Crimes and Enforcement Network, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (2016).

[3] See e.g. 31 C.F.R. § 1020.320(e).

[4] See Mark A. Rush and Joseph A. Valenti, What Companies Can Learn from Cybersecurity Resources in Pittsburgh (2015). The Advisory also points out that "the recently enacted Cybersecurity Act of 2015, also known as the Cybersecurity Information Sharing Act (CISA), does not change any SAR-reporting requirements under the BSA, SAR confidentiality rules, or the safe harbor protections under section 314 of the USA PATRIOT Act."

[5] Mark A. Rush, Thomas C. Ryan, Joseph A. Valenti, and Samuel P. Reger, Treasury Department Issues Cybersecurity Checklist for Financial Institutions: What Might Apply to Your Financial Services Company? (2015).

KEY CONTACTS



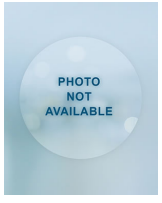
MARK A. RUSH
PARTNER

PITTSBURGH, WASHINGTON, DC
+1.412.355.8333
MARK.RUSH@KLGATES.COM



STANLEY V. RAGALEVSKY
OF COUNSEL

BOSTON
+1.617.951.9203
STANLEY.RAGALEVSKY@KLGATES.COM



REBECCA H. LAIRD
SENIOR OF COUNSEL

WASHINGTON, DC
+1.202.778.9038
REBECCA.LAIRD@KLGATES.COM

©2005-2026 K&L Gates LLP. All Rights Reserved.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.