FinCEN Issues Guidance on Cybersecurity

By Patty P. Tehrani
Lawyer and Founder of Policy Patty Toolkit

The cybersecurity regulations keep coming. Following New York's proposed regulation on cybersecurity, and notice from banking regulators on proposed cybersecurity rules, the Financial Crimes Enforcement Network (FinCEN) has issued an advisory and related FAQ.

The advisory includes key definitions relevant to cyber-related incidents 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.
• 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.

The advisory explains how BSA requirements apply to cyber-events, cyber-enabled crime, and cyber-related information with guidance on:
• reporting cyber-enabled crime and cyber-events through SARs;
o consider all available information surrounding the cyber-event, including its nature and the information and systems targeted;
o determine monetary amounts involved in the transactions or

attempted transactions (should consider in aggregate the funds and assets involved);
o know other cyber-related SAR filing obligations required by their functional regulator;
• including relevant and available cyber-related information (examples provided – IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information) in SARs to:
o provide complete and accurate information, including relevant facts, to the extent available:
 description and magnitude of the event;
 known or suspected time, location, and characteristics or signatures of the event;
 indicators of compromise;
 relevant IP addresses and their timestamps;
 device identifiers;
 methodologies used; and
 other information the institution believes is relevant;
o refer to the FAQs for additional information on reporting cyber-related information in SARs;
• collaborating internally between BSA/Anti-Money Laundering (AML) units and other units to identify suspicious activity to:
o make sure to internally share relevant information from across the organization to help reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units;
o use cyber-related information to:
 help identify suspicious activity and criminal actors;
 develop a more comprehensive understanding of their BSA/AML risk exposure;
 use information provided by BSA/AML units to help the institution guard against cyber-events and cyber-enabled crime;
 provide for more comprehensive and complete SAR reporting;
• sharing information among financial institutions to guard against and report money laundering, terrorism financing, and

cyber-enabled crime to:
o identify threats, vulnerabilities, and criminals; and
o note the extension of Section 314(b) of the USA PATRIOT Act as a safe harbor from liability to financial institutions—after notifying FinCEN and satisfying certain other requirements— to encourage information sharing.
The supplemental FAQs provide additional guidance on reporting obligations for cyber events and cover the following questions:
• What information should a financial institution include in SARs when reporting cyber-events and cyber-enabled crime?
• How should a financial institution complete SARs when reporting cyber-events and cyber-enabled crime
• How should cyber-events and cyber-enabled crime be characterized in SARs?
• How does a financial institution report numerous cyber events in SARs?
• Is a financial institution required to file SARs to report continuous scanning or probing of a financial institution's systems or network?
• Should a SAR be filed in instances where an otherwise reportable cyber-event is unsuccessful?
• Does FinCEN now require financial institutions' BSA/AML units to have personnel/systems devoted to cybersecurity?
• Are BSA/AML personnel now required to be knowledgeable on cybersecurity and cyber-events?
• Can financial institutions use Section 314(b) of the USA PATRIOT Act to share cyber-event and cyber-enabled crime information with other financial institutions
Note: These new FAQs replace prior guidance provided by FinCEN.

FinCEN hopes the guidance will help reduce cyber risks for financial institutions as serve as a reminder on:
• their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime;
• how BSA reporting helps U.S. authorities combat cyber-events

and cyber-enabled crime;
• compliance with BSA requirements or other regulatory obligations for financial institutions does not absolve them from having to comply with federal and state notice/reporting requirements and guidance on cyber-related incidents;
• encouraging collaboration:
o within financial institutions—between employees combating cyber-crime and employees combating money laundering;
o information sharing between financial institutions to again more effectively combat cyber-crime; and
• filing a Suspicious Activity Report (SAR) does not relieve it from any other applicable notice requirements of events impacting critical systems and information or of disruptions in their ability to operate.

Note: Under the Bank Secrecy Act, financial institutions must file SARs to report suspicious activity.