Financial Services Update: FinCEN Issues Advisory Regarding SAR Filing in Connection with Cyber-Events

October 26, 2016

In light of the proliferation of cybercrime affecting consumers and financial institutions, on October 25, 2016, the FinCEN (Financial Crimes Enforcement Network) issued an advisory and FAQ to U.S. financial institutions regarding their Bank Secrecy Act (BSA) obligations related to cyber-events and cyber-enabled crime. The advisory is targeted at four specific areas:

1. Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);

2. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) 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, terrorism financing, and cyber-enabled crime.

In this advisory, FinCEN introduces three concepts: the cyber-event, cyber-related crime, and cyber-related information. *Cyber-event* is defined as an "attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information." *Cyber-enabled crime* is defined as "illegal activities (e.g., fraud, money laundering, and identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers." Finally, *cyber-related information* is defined as "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."

Cyber-events can involve fraud, identity/credential theft, and misappropriation of funds, or it can involve illicit proceeds from events such as a ransomware attack or the theft of credit card information. A financial institution is required to report a suspicious transaction of $5,000 or more. If a financial institution knows or suspects that a cyber-event was part of a transaction at the financial institution, the cyber-event should be considered an attempt to conduct a suspicious transaction. In determining whether a cyber-event should be reported, a financial institution should consider all available information, including the information and systems targeted, and the aggregate funds and assets involved. Financial institutions will also need to comply with any other SAR obligations required by their functional regulator.

FinCEN also encourages financial institutions to report other types of cyber-events that may not otherwise require filing of a SAR, such as a distributed denial of service attack (DDoS). The advisory further encourages financial institutions to include available cyber-related information when filing either a voluntary or required SAR. SARs involving cyber-events should include (to the extent available):

- Description and magnitude of the event
- Time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

For additional information, please refer to the FinCEN advisory and the FAQ.

If you have further questions about your institution's obligations related to cyber-events and cyber-enabled crime, please contact George Meinz.