VORYS

Publications

FinCEN Proposes New Reporting Requirements for Cyber-Events

Related Services

Technology Transactions

Related Industries

Financial Institutions

AUTHORED ARTICLE | Summer 2017

Published in the Summer 2017 issue of *The Bankers' Statement*

The Financial Crimes Enforcement Network (FinCEN) earlier this year issued a proposed rule to change certain data fields on its Suspicious Activity Report (SAR) form. While most of the proposed changes would alter the list of violations that required a SAR, several fields are proposed relating to "cyber-events." These proposed changes to the SAR form follows the Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime issued on October 25, 2016, by FinCEN (the advisory), which advised financial institutions to:

1. Report cyber-enabled crimes and "cyber-events" through SARS

2. Include relevant cyber-related information like IP addresses, timestamps and device identifiers in SARs

3. Have in-house BSA/anti-money laundering units and cybersecurity units coordinate to identify suspicious activity

4. Share cyber-related information among financial institutions to better protect against money laundering and cyber-related crime

Pursuant to the advisory, a "cyber-event" is defined broadly to include any attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources or information.

Traditionally, SARs have pertained to misuse of a financial institution's accounts by customers or employees. The creation of the "cyber-event" category requires institutions to detect and report a variety of potentially suspicious cyber incidents, whether they are directed at customer accounts, or the bank itself. Although the advisory states that it is "not intended to, and does not, create any new obligation or expectation requiring financial institutions to collect cyber-related information as a matter of course," under the proposed SAR form, "other" cyber-events and accompanying cyber-related information is to be reported as well.

The scope of information requested through the proposed SAR form is significant, and is projected to have a significant impact on financial institutions and their compliance teams. For example, the proposed SAR form has specific instructions to report the use of malware, suspicious email addresses or file names, which may include simple phishing emails. Given the receipt of these virtually every day by many institutions, requirements to report all of these could overwhelm the bank's reporting staff as well as FinCEN.

Written comments to the proposed revisions to the SAR form were due April 3, 2017, and comments were received from large and small financial institutions and their representative organizations. Many commentators noted the burden that the proposed SAR form changes would create, as well as requested guidance on FinCEN's expectations for the data fields, particularly in light of rapidly changing techniques and technology. Wells Fargo, for example, noted that "there are technology challenges and significant resource burdens when attempting to identify, capture and report" cyber-event information, and that in an area where "technology, and schemes change at a rapid pace" requested additional guidance from FinCEN on its expectations for cyber-event reporting. Similarly, the National Association of Federally-Insured Credit Unions (NAFCU), cautioned FinCEN that the changes "remain a burden to implement for many of our smaller members," and recommended that FinCEN consider providing a separate methodology outside of the current SAR process to fulfill cyber-event reporting requirements by IT departments directly to FinCEN, "mainly due to the unique, evolving and technical nature of each cybercrime." This request acknowledges the challenge that many BSA/AML compliance staff may face in that they may lack the necessary technical knowledge and skills necessary to helpfully report and explain cyber-events to law enforcement.

While a final decision on the proposed changes to SAR reporting is pending, it is important for financial institutions to begin evaluating their compliance programs to respond to these potential changes, as they may take signification time and resources to implement. Given that violations pertaining to SAR reporting carry the risk of massive fines and criminal prosecution, any impact on cybersecurity compliance of the proposed SAR form should be evaluated fully.

Please contact your Vorys attorney with any questions about these new reporting requirements.