CARLTON FIELDS

Banks to Broaden Reporting of Suspicious Cyber Activity; Regulators Propose "Enhanced" Cybersecurity Standards for Large Financial Institutions

November 22, 2016

The fourth quarter of 2016 has seen an uptick in regulatory activity respecting the financial services sector in the cybersecurity space, both at the state level as previously discussed (here) and on the federal level. Indeed, just last month, the federal government: (1) issued an advisory concerning the types of cybersecurity events financial institutions are required and encouraged to report; and (2) announced that "enhanced" cybersecurity standards for larger institutions are imminent. Each of these developments is discussed in greater detail below. **FinCEN Encourages Banks to Broadly Report on Suspicious Cyber Activity** In October 2016, the Financial Crimes Enforcement Network (FinCEN), an agency of the Treasury Department, issued a formal advisory that addressed the types of cyberattacks or "cyber events" banks are required to report via Suspicious Activity Reports (SARs). *See* FIN-2016-A005 Advisory. Financial institutions are already required to report suspicious banking activity,

including suspicious cyber-related activity, to federal regulators under the Bank Secrecy Act and other anti-money laundering laws. Failing to report such suspicious activity can result in civil or criminal penalties, including heavy fines and regulatory restrictions. To aid banks in that endeavor, FinCEN identifies the types of cyber-related suspicious activity banks are required to report. The advisory explains that banks are required to report cyber incidents involving unauthorized access, or attempts to access, electronic systems or those involving the use of services or resources to conduct unauthorized transactions – such as through use of malware intrusions, ransomware, or other data breaches. Notably, it is not necessary that an actual unauthorized transaction occur to trigger the reporting requirement. Banks are required to report cyber events where $5,000 or more of customer funds are put at risk, or where the customer information sought is reasonably suspected to have been targeted to affect transactions involving/aggregating to $5,000. Banks are also encouraged to report suspicious cyber activity, regardless of the amount at risk, when the event is significant enough to disrupt banking activities – even if the event did not affect any transactions – such as a DDoS (distributed denial of service) attack on the bank's website that temporarily takes it down. The SAR report to FinCEN should include all relevant cyber-event data, such as IP addresses with timestamps, device identifiers, knowledge on methodologies used, and virtual-wallet information. FinCEN uses this information to initiate investigations, identify criminals, and disrupt criminal networks/operations. Significantly, the filing of a SAR for a cyber-event does not relieve the financial institution of the need to report data breaches, such as where required by state data breach notification laws. With this formal advisory, the federal government is sending a clear message that it wants to broaden the scope of the type of information that financial institutions are required, if not encouraged, to include in suspicious cyber activity SARs. For further guidance, financial institutions are encouraged to review FinCEN's FAQs that correspond with the formal advisory. **Regulators Propose Enhanced Cybersecurity Standards for Large Financial Institutions, Invite Public Comment** Also in October 2016, the Board of Governors of the Federal Reserve Board (Federal Reserve Board), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) (collectively, "Regulators") released a joint advance notice of proposed rulemaking (ANPR) inviting public comment on enhanced cyber risk management standards for "large and interconnected entities" under their supervision and services those entities receive from third-party providers.

> **Covered Entities and Services[1]**

If the enhanced standards are implemented as proposed in the ANPR, the following entities will be covered:

- All U.S. bank holding companies with total consolidated assets of $50 billion or more;
- The U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more;
- All U.S. savings and loan holding companies with total consolidated assets of $50 billion or more; and

- Subsidiaries of depository institution holding companies (other than depository institutions supervised by the OCC and FDIC) (collectively, "Covered Entities").

Third-party service providers will be covered in relation to services they provide to Covered Entities or, "Covered Services." Nonbank financial companies and certain financial market utilities and financial market infrastructures may be covered. Community banks will not be covered.

> **The Proposed Enhanced Standards[2]**

Five categories of Enhanced Standards are proposed:

1. Cyber risk governance standards would require Covered Entities to develop "an enterprise-wide cyber risk management strategy" and a "supporting framework of policies and procedures" to implement the strategy that is approved by a board of directors or board committee. Importantly, senior management would be accountable for "establishing and implementing appropriate policies consistent with the strategy," and keeping the board informed concerning cyber risk exposure and risk management practices "on an ongoing basis" and "independent of business line management."

2. Cyber risk management standards would require Covered Entities to integrate cyber risk management into the responsibilities of at least three independent functions including the business unit, independent risk management, and audit functions. Business units would be required to assess cyber risks associated with the day-to-day activities of the Covered Entities and report the information to senior management "on an ongoing basis" and "in a timely manner" so risks and incidents can be addressed and responded to by senior management as they develop. Independent risk management would be required to analyze cyber risks across the enterprise, continually assess overall exposure and "promptly notify the [Covered Entity's] CEO and board of directors, as appropriate, when its assessment of a particular cyber risk differs from that of a business unit, as well as of any instances when a unit of the covered entity has exceeded the entity's established cyber risk tolerances." The audit function would be required to assess whether a Covered Entity's cyber risk management framework complies with applicable laws and regulations and provides an evaluation of the adequacy of compliance with the Covered Entity's cyber risk management framework; and cyber risk policies, procedures and processes.

3. Internal dependency management standards would require Covered Entities to continually assess and improve their effectiveness in reducing cyber risks associated with their "business assets," which are identified in the ANPR as the Covered Entities' workforce, data, technology, and facilities relied upon to deliver services, and the communication flows among them.

4. External dependency management standards would require Covered Entities to continually assess and improve their effectiveness in reducing cyber risks associated with their "external dependencies" or their "relationships with outside vendors, suppliers, customers, utilities, and other external organizations and service providers" relied upon to deliver services, and the communication flows among them.

5. Incident response, cyber resilience, and situational awareness standards would require Covered Entities "to plan for, respond to, contain, and rapidly recover from disruptions caused by cyber incidents"; "to be capable of operating critical business functions in the face of cyber-attacks"; and to "establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze, and respond to changes in the operating environment."

> **A "Tiered Approach" and Additional "More Stringent" Standards**

The Regulators propose a "tiered approach" under which the Enhanced Standards are applied to all systems of Covered Entities with "an additional, higher set of expectations" applying to "sector-critical systems." "Sector-critical systems" are described as those systems of Covered Entities that "due to their extensive interconnectedness to other financial entities could have a material impact on financial stability if significantly disrupted."[3] Regulators will integrate the Enhanced Standards into their existing supervisory programs.[4]

> **No Indication as to Timing**

Public comment on all aspects of the ANPR is invited until January 17, 2017. A more detailed proposal will be developed and public comment will be invited once more before any final rule is adopted. The ANPR gives no indication when Enhanced Standards might take effect.

> **Why More Standards?**

In the ANPR, Regulators acknowledge the U.S. financial system is interconnected such that a cyber incident or failure at one interconnected entity may impact the safety and soundness of that entity, other financial entities, and potentially the financial system as a whole.[5] Increased dependence on technology by financial institutions increases the opportunities for cyber attacks that could potentially undermine the financial system. Enhanced cybersecurity standards for the nation's largest financial institutions, which also apply to services provided to those institutions by third-party service providers, are designed to "increase the operational resilience of [Covered Entities] and reduce the impact on the financial system in case of a cyber event experienced by one of these entities."[6] It seems fairly certain 2017 will mean more regulatory requirements and associated compliance costs for large financial institutions and their third-party service providers. ---

[1] ANPR at pg. 13-15.
[2] ANPR at pg. 21-40.
[3] ANPR at pg. 7-8, 17-21 .
[4] ANPR at pg. 8-13.
[5] ANPR at pg. 6-8.
[6] ANPR at pg. 1-2.

Related Practices

Consumer Finance
Cybersecurity and Privacy
Financial Services Regulatory