Client Alert: Federal Banking Regulators and NHTSA Release Cybersecurity Guidance

Related Attorneys

Scott M. Guttman

Related Services

Data Strategy, Privacy and Security

Related Industries

Financial Institutions

Transportation and Logistics

CLIENT ALERT | 11.4.2016

The past few weeks have seen a flurry of activity in the cybersecurity arena – and not just from the intruders, such as those who orchestrated the massive distributed denial of service (DDoS) attack that temporarily took down PayPal, Twitter and others. In an effort to bolster cybersecurity and protect against cybercrime for financial institutions, the Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), announced proposed enhanced cybersecurity standards. Similarly, the Federal Financial Institutions Examination Council (FFIEC) published a Frequently Asked Questions Guide on its cyber security assessment tool. Moreover, the US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) also issued cybersecurity guidance for motor vehicles. Each of these is briefly discussed below.

Enhanced Cyber Risk Management Standards for Financial Institutions

On October 19, 2016, just weeks after the New York Department of Financial Services announced its draft cybersecurity regulation, three federal banking regulatory agencies – the Board, the FDIC, and the OCC – issued an advance notice of proposed rulemaking (ANPR) regarding enhanced cybersecurity risk-management standards aimed at increasing the operational resilience of regulated entities and reducing the impact on the financial system in the event of a cyber-event. These proposed standards apply to (i) depository institutions and depository institution holding companies with total consolidated assets of $50 billion or more, (ii) the U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more, and (iii) financial market infrastructure companies and nonbank financial companies supervised by the Board (collectively, covered entities). The standards would not, however, apply to community banks.

The enhanced standards are organized into five categories: (1) cyber risk governance; (2) cyber risk management; (3) internal dependency management; (4) external dependency management; and (5) incident

response, cyber resilience, and situational awareness. The banking agencies also proposed a two-tiered approach to address the interconnectedness of financial entities. Under this approach, the proposed enhanced standards would apply to all covered entities, and additional, more stringent expectations (*i.e.*, sector-critical standards) would apply to those covered entities' systems that are critical to the financial sector. These sector-critical standards would require covered entities to substantially mitigate the risk of disruption due to a cyber-event impacting their sector-critical systems.

Vendor management continues to be a point of interest by the banking regulators as the proposed standards address the need for more stringent cybersecurity requirements for third-party services providers as well as nonbank financial companies that are supervised by the banking regulators, such as payments processors. The proposed enhanced standards also call for more cybersecurity oversight from boards of directors and senior management, noting that the banking regulators are considering whether they should mandate bank board members have "adequate expertise" in cybersecurity.

Comments on the ANPR may be submitted until January 17, 2017. No timeframe has been set at this time for when these standards may take effect.

Cybersecurity Assessment Tool FAQs

The FFIEC also recently released a set of answers to frequently asked questions (FAQ) about the Cybersecurity Assessment Tool (Assessment) in response to questions and requests to clarify points of the Assessment. The Assessment was released last summer to help financial institutions identify their risks and assess their cybersecurity preparedness. First and foremost, the seven page FAQ confirms that the Assessment is voluntary. The FAQ also explains (i) that the Assessment may be used as a resource for management's "oversight of third parties as part of the institution's comprehensive third-party management program;" (ii) how the Assessment aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework; and (iii) that the FFIEC does not intend to release an automated version of the Assessment at this time. The FAQ also specifically addresses Inherent Risk Profiles (as determined in part one of the Assessment) and how these profiles should align with the institution's maturity level within each of the five cybersecurity domains.

Automobile Industry Cybersecurity Guidance

On the heels of the banking regulators' announcements, on October 24 the NHTSA released proposed guidance on improving motor vehicle cybersecurity. To better protect vehicles from malicious cyber-attacks and unauthorized access, the guidance (i) focuses on layered solutions to ensure vehicle systems are designed to take appropriate and safe actions, even when an attack is successful; (ii) recommends risk-based prioritized identification and protection of critical vehicle controls and consumers' personal data; and (iii) recommends that companies should consider the full life-cycle of their vehicles and facilitate rapid response and recovery from cybersecurity incidents. This guidance also highlights the importance of making cybersecurity a top leadership priority for the automotive industry, and suggests companies allocate appropriate and dedicated resources to cybersecurity as well as enable seamless and direct communication channels though organizational ranks related to vehicle cybersecurity matters. NHTSA is seeking public comments on the proposed guidance for 30 days.

These developments demonstrate that regulatory emphasis and expectations regarding cybersecurity and cybersecurity risk management continue to increase. For questions regarding these proposed cybersecurity regulations or other issues related to cybersecurity, contact Heather Enlow-Novitsky, Scott Guttman or your Vorys attorney.