Cullen | Dykman

Guidance Issued on Safeguarding the Cybersecurity of Interbank Messaging and Payment Networks

July 22, 2016

The Federal Financial Institutions Examination Council ("FFIEC") has issued guidance to financial institutions to "actively manage the risk associated with interbank messaging and wholesale payment networks ("Networks")" as a result of recent cyber-attacks. The expectation is for financial institutions to review, update and improve their IT risk management and cybersecurity practices in conjunction with an assessment of the risks associated with the Networks to avoid such attacks.

In April 2016, the Bangladesh central bank was the victim of a well-publicized attack in which it was reported that $81 million was stolen from an apparent hack into the software from the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") financial platform. In light of this incident and other recent cyber-attacks, which aim to exploit "vulnerabilities and unauthorized entry through trusted client terminals running messaging and payment networks," the FFIEC is calling for financial institutions to follow the guidelines set forth in its *IT Examination Handbook* as well as the guidelines put forth by the Networks themselves.

Cybersecurity and the Networks

The National Institute of Standards and Technology defines cybersecurity as "the process of protecting information by preventing, detecting and responding to [cyber] attacks." Most recently, cyber-attacks have been targeting these Networks and in doing so have demonstrated the capability to:

- Compromise a financial institution's wholesale payment origination environment, bypassing security controls;
- Obtain and use valid operator credentials with the authority to create, approve and submit messages;
- Employ a sophisticated understanding of funds transfer operations and operational controls;
- Use highly customized malware to disable security logging and reporting, as well as other operational controls to conceal and delay detection of fraudulent transactions; and
- Transfer stolen funds across multiple jurisdictions quickly to avoid recovery.

These Networks, such as Fedwire Funds Services ("Fedwire") and Clearing House Interbank Payment Systems ("CHIPS"), are being targeted because of the immense value of the daily transactions associated with these

systems. As a whole, these Networks are generally used to transfer the funds needed to purchase, sell or finance large value securities, settle real estate transactions, disburse or repay loans, and settle interbank purchases. Since the Networks are used frequently by financial institutions for large value transactions, cyber-attacks are becoming more common and are putting financial institutions at risk of financial loss and regulatory non-compliance.

Risk Mitigation

In order to help mitigate the risks of cyber-attacks on the Networks, the FFIEC suggests that financial institutions "use multiple layers of security controls to establish lines of defense." The FFIEC has proposed that financial institutions take the following steps in order to help prevent cyber-attacks and mitigate the risks when, and if, they do take place:

- Conduct ongoing information security risk assessments (including considering new and evolving threats to online accounts and adjusting customer authentication, layered security, and other controls in response to identified risks accordingly);
- Perform security monitoring, prevention and risk mitigation (ensuring protection and detection systems are up-to-date and firewalls are configured properly);
- Protect against unauthorized access (by limiting the number of credentials with elevated privileges across the institution and the ability to easily assign elevated privileges to access critical systems);
- Implement and test controls around critical systems regularly (including limiting the number of sign-on attempts when accessing critical systems);
- Manage business continuity risk;
- Enhance information security awareness and training programs; and
- Participate in industry information-sharing forums (such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the U.S. Computer Emergency Readiness Team (US-CERT)).

Additional Information

The FFIEC guidance was issued on June 7, 2016, and may be accessed through the following link: http://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf.

If you have any questions regarding the guidance, please feel free to contact Kevin Patterson at 516-296-9196 or via email at kpatterson@cullenanddykman.com, Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com, or Jeff Fowler at 516-296-9134 or via email at jfowler@cullenanddykman.com.

Practices

- Banking and Financial Services
- Regulatory and Compliance

Industries

- Financial Institutions

Attorneys

- Kevin Patterson
- Joseph D. Simon