
**Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation**

August 17, 2016

The Honorable Carolyn B. Maloney
Ranking Member
Subcommittee on Capital Markets and
Government Sponsored Enterprises
House of Representatives
Washington, D.C. 20515

Dear Ranking Member Maloney:

Thank you for your letter of May 23, 2016, to the Board of Governors of the Federal Reserve System (Federal Reserve Board), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC), collectively the “agencies,” regarding recent events involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Your letter expressed concern about the recent reports of cyber-attacks at foreign institutions that have exploited payment systems, and requested information about the steps the agencies have taken, or plan to take, to ensure that U.S. banks maintain effective controls for interbank messaging and payment networks. The safety and soundness of the financial industry is dependent on secure payment systems, and the agencies continue to focus on information security and payment systems risk as part of our ongoing supervisory oversight processes.

The agencies have taken a number of steps to address information security concerns related to the SWIFT messaging network. In coordination with the Federal Financial Institutions Examination Council (FFIEC)¹ members, the agencies issued a joint statement on June 7, 2016, *Cybersecurity of Interbank Messaging and Payment Networks*,² to emphasize the steps financial institutions should be taking to actively manage the risks associated with interbank messaging and wholesale payment networks. The joint statement stresses that financial institutions should review risk management practices and controls related to information technology systems and payment networks including risk assessment; authentication, authorization and access controls; monitoring and mitigation; fraud detection; and incident response.

Risk management practices and controls also are set forth in the FFIEC’s *Information Technology (IT) Examination Handbook*, which describes supervisory expectations and examination standards for financial institution technology operations. As part of this handbook, specific booklets outline supervisory expectations and specific examination procedures that

¹ The FFIEC was established in March 1979 to prescribe uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. The Council consists of the following: Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Consumer Financial Protection Bureau; Comptroller of the Currency; National Credit Union Administration; and the State Liaison Committee.

² See: <https://www.ffiec.gov/press/pr060716.htm>.

address information security, wholesale payment systems, and retail payment systems. Furthermore, financial institutions that rely on payment systems infrastructure, such as SWIFT, are required to adhere to policies and standards required by the payment network.³

In addition to the joint statement, each of the agencies is taking steps to reinforce with examiners key controls and risk management practices that should be incorporated in supervision activities. Many of the largest and most critical institutions to the U.S. banking industry that use international payment messaging systems, such as SWIFT, have dedicated examination teams conducting ongoing supervision throughout the year. These examination teams include subject matter experts dedicated to reviewing information security, payment systems, and operations risk and maintain ongoing communication with bank management teams to address security events and assure that the institutions maintain appropriate monitoring and controls for these threats.

The Federal Reserve, as a member of the group of central banks participating in the cooperative oversight arrangement for SWIFT (led by the National Bank of Belgium), has staff actively engaged in monitoring SWIFT's response to these developments.⁴ In addition, on May 25, 2016, the Federal Reserve Board issued an internal alert to its supervision teams of banks and financial market utilities⁵ that are known SWIFT customers to make sure institutions were adequately mitigating the threats.

The OCC is drafting specific guidance for examiners on interbank messaging and wholesale payment systems risk management. This guidance provides examiners with specific information on key controls and risk management practices that should be assessed as part of supervisory oversight activities and references the existing supervisory standards and tools for examining interbank messaging and wholesale payment systems. As part of ongoing supervision activities, the OCC's onsite examination teams regularly address emerging issues, such as the recent reports of cyber-attacks involving SWIFT.

The FDIC provided information first to its examiners and then to the institutions that it supervises. On May 18, 2016, the FDIC provided examiners with an internal alert on the SWIFT threat and instructions for conducting an expanded review of cyber controls related to SWIFT or any wholesale payment system at future examinations. On June 1, 2016, the FDIC sent technical guidance to FDIC-supervised institutions via its private communication system on detecting and mitigating the threat. These documents included: 1) the Department of Homeland Security and Federal Bureau of Investigation Joint Analysis Report on Recommended Mitigations for Institutions with Connections to Payment Messaging Systems; and 2) National Cybersecurity and Communications Integration Center/United States Computer Emergency Readiness Team

³ Financial institutions are also subject to any applicable state laws incorporating the requirements of Article 4A of the Uniform Commercial Code, which governs funds transfers.

⁴ For additional information about SWIFT oversight, see: <https://www.swift.com/about-us/organisation-governance/oversight>.

⁵ "Financial market utilities (FMUs) are multilateral systems that provide the infrastructure for transferring, clearing, and settling payments, securities, and other financial transactions among financial institutions or between financial institutions and the system."

https://www.federalreserve.gov/paymentsystems/designated_fm_u_about.htm.

Malware Initial Findings Report on malicious software used to target the Alliance Access application developed by SWIFT.

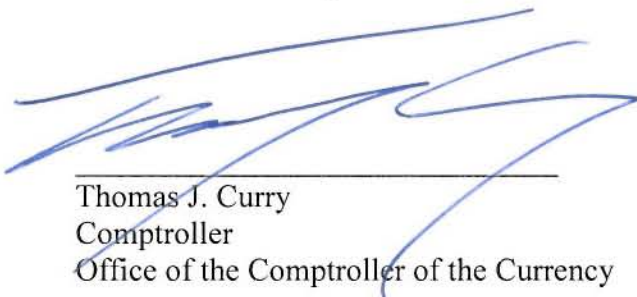
Finally, as a general matter, the agencies are continuing to heighten our focus on cybersecurity risks and controls for U.S. financial institutions as part of our ongoing supervisory processes. On June 30, 2015, the FFIEC released its Cybersecurity Assessment Tool to help institutions identify their risks and assess their cybersecurity preparedness. The agencies continue to closely monitor cybersecurity threats to the U.S. financial industry and reassess the adequacy of current cybersecurity standards and guidance.

Thank you again for your letter and your interest in ensuring continued vigilance to protect the nation's financial system from harmful cyber-attacks.

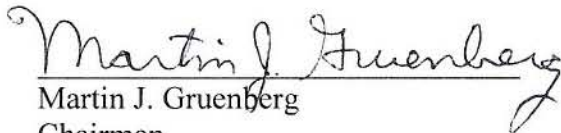
Sincerely,



Janet L. Yellen
Chair
Board of Governors of the
Federal Reserve System



Thomas J. Curry
Comptroller
Office of the Comptroller of the Currency



Martin J. Gruenberg
Chairman
Federal Deposit Insurance Corporation