United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

May 19, 2016

William C. Dudley
President and Chief Executive Officer
The Federal Reserve Bank of New York
33 Liberty Street
New York, NY 10045

Dear Mr. Dudley:

I write today to request information about recent cyberattacks involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a provider of secure messaging services for financial institutions.

In February 2016, an anonymous group of cyber criminals reportedly posed as the Central Bank of Bangladesh and used the SWIFT system to fraudulently transfer $81 million from an account at the Federal Reserve Bank of New York to accounts in the Philippines. According to press reports, these criminals exploited weak cybersecurity protections at the Central Bank of Bangladesh to create fully authenticated transfer orders and then used sophisticated malware to hide evidence of the transaction.

Most recently, it was reported that cyber criminals also used the SWIFT system to attack the Tien Phong Bank in Vietnam. In a May 13, 2016 letter to its users, SWIFT apparently warned that this attack was part of a "wider and highly adaptive campaign targeting banks" and that the "attackers clearly exhibit a deep and sophisticated knowledge of specific operation controls within the targeted banks…."

It is my understanding that there is no evidence of any attempt to penetrate Federal Reserve systems or that any Federal Reserve systems were compromised in connection with these recent incidents. However, these cyberattacks raise important questions about the security of the SWIFT system and the ability of its members to prevent future attacks. Congress has a responsibility to continue to strengthen our nation's cybersecurity, including ensuring that the system used by our banks to engage in cross-border transactions is secure. Only by staying a step ahead of these cyber threats can we ensure the security of our financial system.

To better understand how the Federal Reserve is addressing these attacks, I ask that you please provide the following information by June 17, 2016:

1. Does the Federal Reserve plan to revise its cybersecurity policies or its own internal control environment in response to these recent attacks? If so, please explain.

2. Cyber criminals reportedly attempted the attack on the Tien Phong Bank several months before the attack on the Central Bank of Bangladesh. What are the protocols and practices of the Federal Reserve Bank of New York for sharing information about cybersecurity threats targeting SWIFT member banks?

3. While SWIFT can advise members on cybersecurity practices, SWIFT does not employ a mechanism to ensure that members adhere to those standards. According to the SWIFT website, "the main instrument for oversight of SWIFT is moral suasion." Has the Federal Reserve provided technical assistance to commercial or foreign central bank end users on the types of technical, operational, managerial, and procedural controls that could best protect the security of the SWIFT network?

4. Please describe the steps the Federal Reserve has taken to coordinate with SWIFT, the Central Bank of Bangladesh, the Department of Homeland Security, the Department of Treasury, and other institutions to strengthen the security of the SWIFT system since the attacks.

I also request that you ensure that a briefing is scheduled with my staff regarding these issues. The Committee's minority staff is authorized to conduct this investigation under the authority of Senate Rule XXV and Senate Resolution 73 (114th Congress). [redacted]

Thank you for your attention to this matter.

With best personal regards, I am

Sincerely yours,

Tom Carper
Ranking Member

cc: The Honorable Ron Johnson
Chairman