CAROLYN B. MALONEY
12TH DISTRICT, NEW YORK

2308 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3212
(202) 225-7944

COMMITTEES:
FINANCIAL SERVICES

GOVERNMENT REFORM

JOINT ECONOMIC COMMITTEE
|SENIOR HOUSE DEMOCRAT|

Congress of the United States
House of Representatives
Washington, DC 20515-3212

DISTRICT OFFICES:

1651 THIRD AVENUE
SUITE 311
NEW YORK, NY 10128
(212) 860-0606

31-19 NEWTOWN AVENUE
ASTORIA, NY 11102
(718) 932-1804

619 LORIMER STREET
BROOKLYN, NY 11211
(718) 349-5972

WEBSITE: maloney.house.gov
Twitter: @RepMaloney

May 23, 2016

The Honorable Janet L. Yellen
Chair
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

The Honorable Thomas J. Curry
Comptroller of the Currency
Office of the Comptroller of the Currency
250 E Street SE
Washington, DC 20219

The Honorable Martin J. Gruenberg
Chairman
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Dear Chair Yellen, Comptroller Curry, and Chairman Gruenberg:

I am writing with regard to the recent news that cyber criminals have, on more than one occasion, successfully stolen banks' SWIFT credentials, and in at least two instances used those stolen credentials to initiate funds transfers through the SWIFT financial messaging system.[1] Repeated instances of fraudulent messages sent through SWIFT threatens to undermine the security and integrity of cross-border financial transactions.

As you know, more than 11,000 financial institutions use SWIFT to send billions of messages every year, which facilitates trillions of dollars of cross-border payments. The security and integrity of SWIFT messages relies on a robust information security environment at both SWIFT and at member banks.[2]

---

[1] *See* SWIFT, *SWIFT Customer Communication: Customer Security Issues* (May 13, 2016), available at: https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues (last accessed May 15, 2016); SWIFT, *SWIFT Customer Communication: Cooperating on Cyber-Security* (May 20, 2016), available at: https://www.swift.com/insights/press-releases/swift-customer-communication_cooperating-on-cyber-security (last accessed May 20, 2016); *see also* Michael Corkery, "Once Again, Thieves Enter Swift Financial Network and Steal," *New York Times* (May 12, 2016) (detailing a second attack at a bank in Vietnam); Katy Burne, "Swift Finds Evidence of Second Malware Attack," *Wall Street Journal* (May 12, 2016) (same); Devlin Barrett and Katy Burne, "Lawsuit Claims Another Global Banking Hack," *Wall Street Journal* (May 19, 2016) (detailing a third attack at a bank in Ecuador).

[2] *See e.g.*, SWIFT, *General Terms and Conditions* § 5.2 ("The customer is responsible at all times for maintaining the confidentiality, integrity, and availability of traffic, message, and configuration data on its SWIFT systems, and on that segment of its connectivity for which SWIFT is not responsible under the SWIFT Contractual Documentation.").

In all three incidents, it appears to have been the banks' security environment, rather than SWIFT's, that was compromised.[3] These incidents led SWIFT to issue a notice to all of its member banks and other users recommending that they "urgently review controls in their payments environments, to all their messaging, payments and ebanking channels."[4] A week later, SWIFT issued another notice to its users reminding them of "their obligations to immediately inform SWIFT of any suspected fraudulent use of their institution's SWIFT connectivity or related to SWIFT products and services."[5]

Importantly, the Bank of England recently ordered U.K. banks to conduct a cybersecurity review in response to the recent attacks, even though no U.K. banks' SWIFT credentials have been stolen in the incidents that have been reported to date.[6] In particular, the Bank of England ordered banks to review whether they are in compliance with the security practices and policies recommended by SWIFT.[7]

While none of the breaches reported to date have involved cyber criminals compromising a U.S. bank's security environment to steal the U.S. bank's SWIFT credentials, I remain deeply concerned about U.S. banks' exposure to these new, sophisticated cyber attacks. In addition, I believe that your agencies can play an important leadership role in the international response to these cyber attacks.

To that end, I respectfully request answers to the following questions:

- What steps have your agencies taken, or what steps do your agencies plan to take, to ensure that the information security environment at U.S. banks that are members of SWIFT are in full compliance with SWIFT's recommended security practices and policies?

- Have your agencies ordered U.S. banks to undertake a cybersecurity review similar to the review ordered by the Bank of England?

- What steps have your agencies taken, or what steps do your agencies plan to take, to ensure that *all* U.S. banks have adequate security measures in place to protect against cyber attacks that involve stolen SWIFT credentials?

---

[3] *See* SWIFT, *SWIFT Customer Communication: Customer Security Issues* (May 13, 2016) ("The modus operandi of the attackers is similar in both cases: (1) Attackers compromise the bank's environment."); Barrett and Burne, "Lawsuit Claims Another Global Banking Hack" (May 20, 2016) ("According to that filing on behalf of Banco del Austro, or BDA, 'For each of the unauthorized transfers, *an unauthorized user, using the Internet, hacked into BDA's computer system* after hours using malware that allowed remote access, logged onto the Swift network purporting to be BDA, and redirected transactions to new beneficiaries with new amounts.'") (emphasis added).

[4] SWIFT, *SWIFT Customer Communication: Customer Security Issues* (May 13, 2016).

[5] SWIFT, *SWIFT Customer Communication: Cooperating on Cyber-Security* (May 20, 2016).

[6] *See* Andrew MacAskill and Jim Finkle, "Exclusive: UK Banks Ordered to Review Cyber Security After SWIFT Heist," *Reuters* (May 18, 2016), available at: http://www.reuters.com/article/us-cyber-heist-bankofengland-idUSKCN0Y92KR (last accessed May 20, 2016).

[7] *Id.*

If you have any questions about this request, please contact Ben Harney on my staff at (202) 225-7944.

Sincerely,

Carolyn B. Maloney
Ranking Member
Subcommittee on Capital Markets and
Government Sponsored Enterprises