LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

May 31, 2016

Mr. William C. Dudley
President
Federal Reserve Bank of New York
33 Liberty Street
New York, NY 10045

Dear Mr. Dudley,

The Committee on Science, Space, and Technology is conducting oversight of a recent security event involving the Federal Reserve Bank of New York (NY Fed). According to numerous press reports, on February 4-5, 2016, approximately $101 million was stolen – by compromising the digital platform referred to as SWIFT Alliance Access server software[1] used to transfer money internationally – from the Bank of Bangladesh (or Bangladesh Bank) accounts at the Federal Reserve Bank of New York.[2] The cyber thieves used malicious code or malware, according to one report.[3] In total, the cyber thieves attempted to steal $1 billion via 35 separate orders. The NY Fed stopped payment on 30 of the orders, $20 million was returned by a Sri Lankan bank because bank staff caught a misspelling in the name of the recipient, and $4.63 million was returned by "one of the [gambling] junket operators in the Philippines."[4] We are writing to request a briefing and information related to the February incident as well as information related to the NY Fed's role in overseeing the Society for Worldwide Interbank Financial Telecommunication or SWIFT.

Recent media reports by *Reuters* and *CNBC* confirm that cyber attackers were able to gain access to SWIFT software by using malware.[5] Specifically, the reports state: "new evidence suggests that hackers manipulated the Alliance Access server software, which banks use to interface with SWIFT's messaging platform, in a bid to cover up fraudulent transfers that had been previously ordered."[6] SWIFT, according to reports, provided a software update to enhance

---

[1] Jim Finkle, *Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued*, REUTERS, Apr. 25, 2016 [hereinafter Finkle, Apr. 25, 2016].
[2] Kim Zetter, *That Insane, $81M Bangladesh Bank Heist? Here What We Know*, WIRED MAGAZINE, May 17, 2016; Syed Zain Al-Mahmood, *Who Stole $100 Million From Bangladesh's Account at the New York Fed?*, WALL ST. J., Mar. 16, 2016; Syed Zain Al-Mahmood & Cris Larano, *From the Fed to the Philippines: Bangladesh's Stolen-Money Trail*, WALL ST. J., Mar. 18, 2016 (noting that a transfer in the sum of $20 million was reversed) [hereinafter Al-Mahmood, Mar. 18, 2016].
[3] Al-Mahmood, Mar. 18, 2016.
[4] Katy Burne & Syed Zain Al-Mahmood, *Accidental Accomplice in Central-Bank Cyberheist: Bankers' Hours*, WALL ST. J., Apr. 9, 2016 [hereinafter Al-Mahmood, Apr. 9, 2016].
[5] Finkle, Apr. 25, 2016
[6] *Id.*

users' security.[7] Weaknesses existed within the computer network of the Bangladesh Bank and based on research done by a third party, cyber criminals were able to exploit these vulnerabilities. Then, the cyber criminals covered their tracks using malware named evtdiag.exe.[8] This malware was sophisticated enough to do the following: change the code of access to the Access Alliance software installed at Bangladesh Bank, giving the hackers access to manipulate records of transfer requests; intercept incoming messages verifying the transfer orders; and even "manipulate account balances on logs to prevent" discovery of the entire operation.[9]

On or about April 25, 2016, SWIFT acknowledged that there were "a number of recent cyber incidents where attackers had sent fraudulent messages over its system."[10] According to *Reuters*, SWIFT sent a notice alerting its partners that this "was not an isolated incident, but one of several recent criminal schemes aimed to take advantage of the global messaging platform used by some 11,000 financial institutions."[11] Cybersecurity experts warn that more attacks could be uncovered as banks review their systems.[12] This is deeply troubling and it is Congress' responsibility to ensure, through its oversight, that the NY Fed is taking all precautions to protect American finances and aggressively execute its own role as overseer of SWIFT. One cybersecurity expert pointed out that a system is "only as safe as the weakest link."[13]

In this case, the Bangladesh Bank's systems appear to have been the weak link. Reports state that Bangladesh Bank's system was "fractured and antiquated," and sources claim that they were using $10 routers and no firewalls.[14] In contrast, American financial institutions employ numerous firewalls and physically separate sensitive systems enclosing them in locked server rooms.[15] According to *Bloomberg*, the Bank of Bangladesh's systems were so poorly protected that a security company hired to investigate the attack found their systems were comprised by no less than three groups of hackers – two of which were nation states.[16] *Bloomberg* also reported that a meeting between SWIFT, the Bank of Bangladesh, and the NY Fed took place on May 10, 2016, to discuss the status of the ongoing investigation into the cyberattack.[17] A statement released after the meeting stated that the attendees "were committed to recovering the proceeds of the fraud, bringing the perpetrators to justice, and working together 'to normalize operations.'"[18] The Committee is interested in learning the status of these initiatives. We

---

[7] *Id.*
[8] *Id.* (citing work done by a team at BAE Systems, a British defense contractor).
[9] *Id.*
[10] Jim Finkle, *Exclusive: SWIFT Warns Customers of Multiple Cyber Fraud Cases*, REUTERS, Apr. 26, 2016 [hereinafter Finkle, Apr. 26, 2016].
[11] *Id.*
[12] *Id.*
[13] Michael Corkery, *Hackers' $81 Million Sneak Attack on World Banking*, N.Y. TIMES, Apr. 30, 2016.
[14] *Id.*
[15] *Id.*
[16] Arun Devnath & Michael Riley, *Bangladesh Bank Heist Probe Said to Find Three Hacker Groups*, BLOOMBERG, May 10, 2016.
[17] *Id.*
[18] *Id.*

request that you or other appropriate officials provide a briefing to Committee staff no later than June 14, 2016.

The question of bringing those responsible to justice is an important one. To date, investigators have not publicly announced significant progress. Their work, however, has dredged up "a colorful cast of characters" as *Bloomberg* points out.[19] Those implicated include casino operators in the Philippines, bank managers, and a Sri Lankan non-profit foundation leader.[20] On May 12, 2016, the *New York Times* reported that SWIFT disclosed a second attack – involving a commercial bank – bearing resemblance to the Bank of Bangladesh attack.[21] In this subsequent incident it was again the links to SWIFT that were exploited. Additionally, there may have been insiders involved. Three days later, Vietnam's Tien Phong Bank admitted to being the second victim of a cyberattack.[22] In that instance, the bank caught the fraudulent SWIFT messages in time to halt a transfer of approximately $1.1 million. The Committee, while concerned about all potential vulnerabilities, is focused on the technology employed by SWIFT and the banks that move money through SWIFT.

Based in Belgium, SWIFT is, according to its website, a "neutral global cooperative," overseen by National Bank of Belgium "together with the G-10 central banks: Bank of Canada, Deutsche Bundesbank,…and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.[23] SWIFT's systems have been used since the 1970s and are "owned and overseen by the world's biggest banks."[24] It maintains a culture of operating in the background and not disclosing any user specific information.[25] In light of the recent cyberattacks on our global financial systems, the Committee believes it is imperative to receive information from the NY Fed about its response, its oversight of SWIFT, the status of the investigation, and any remedial steps taken to address vulnerabilities.

To assist in the Committee's evaluation of the NY Fed's response to the February cyberattack, please provide the following documents and information for the time frame June 1, 2015, to the present, as soon as possible, but by no later than noon on June 14, 2016:

1. All documents and communications referring or relating to the February 4-5, 2016, cyberattack involving the Bank of Bangladesh.

---

[19] *Id.*
[20] *Id.*
[21] Michael Corkery, *Once Again, Theives Enter Swift Financial Network & Steal*, N.Y. TIMES, May 12, 2016 [hereinafter Corkery, May 12, 2016].
[22] Eamon Javers, *Vietnam's Tien Phong Bank Says it was Second Bank Hit by SWIFT Cyberattack*, CNBC report, May 15, 2016.
[23] Society for Worldwide Interbank Financial Telecommunication website, Organisation and Governance, Oversight *available at* https://www.swift.com/about-us/organisation-governance/oversight#topic-tabs-menu (last visited May 19, 2016).
[24] Corkery, May 12, 2016.
[25] *Id.*

2. All documents and communications related to security of the NY Fed's SWIFT system(s).

3. All documents and communications related to any oversight, audits, or investigative reports the NY Fed has conducted related to SWIFT's cybersecurity.

4. All documents and communications related to any review conducted by the NY Fed of its own information technology system(s) in the days following the Bank of Bangladesh cyberattack.

The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology which develops cybersecurity standards and guidelines to support the implementation of and compliance with FISMA as set forth in House Rule X. Additionally, the Committee has general oversight and investigative authority on all matters relating to competitiveness, technology, standards, and innovation.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment provides information regarding producing documents to the Committee.

If you have any questions about this request, please contact Committee staff at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

Barry Loudermilk
Chairman
Subcommittee on Oversight

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member
The Honorable Don Beyer, Ranking Member, Subcommittee on Oversight

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents, in unredacted form, that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.

2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.

3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.

4. Documents produced in electronic format should also be organized, identified, and indexed electronically.

5. Electronic document productions should be prepared according to the following standards:

   (a) The production should consist of single page Tagged Image File ("TIF"), or PDF files.

   (b) Document numbers in the load file should match document Bates numbers and TIF or PDF file names.

   (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.

8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.

9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.

10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.

11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.

12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.

13. In complying with this request, be apprised that the U.S. House of Representatives and the Committee on Science, Space, and Technology do not recognize: any of the purported non-disclosure privileges associated with the common law including, but not limited to, the deliberative process privilege, the attorney-client privilege, and attorney work product protections; any purported privileges or protections from disclosure under the Freedom of Information Act; or any purported contractual privileges, such as non-disclosure agreements.

14. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.

15. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.

16. Unless otherwise specified, the time period covered by this request is from June 1, 2015 to the present.

17. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.

18. All documents shall be Bates-stamped sequentially and produced sequentially.

19. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 324 of the Ford House Office Building.

20. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive

documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Schedule Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.

3. The terms "and" and "or" shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

4. The terms "person" or "persons" mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.

6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.