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

April 20, 2016

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

Dear Mr. Gruenberg,

The Committee on Science, Space, and Technology is continuing its oversight of a recent security event at the Federal Deposit Insurance Corporation (FDIC).[1] Since writing to you on April 8, 2016, the Committee became aware that the FDIC initially withheld reporting a recent security incident to Congress as required by the Federal Information Security Modernization Act of 2014 (FISMA) until prompted to do so by the FDIC Office of Inspector General (OIG). The breach at issue involved an employee who copied sensitive FDIC information for over 10,000 individuals onto a portable storage device prior to separating from employment at the FDIC.[2] Given that the facts surrounding this additional security incident are strikingly similar to the incident about which I previously wrote to you and because the FDIC apparently withheld information from Congress about the incident, the Committee remains concerned that the FDIC does not have the necessary controls in place to prevent and respond appropriately to security breaches.[3] To assist in the Committee's oversight of this matter, the Committee requests that the FDIC be prepared to discuss the FDIC's response to this incident at a briefing scheduled for later this week.

In October 2015, an FDIC employee who was in the process of separating from agency employment copied personal information and customer data for over 10,000 individuals onto a personal portable storage device.[4] On October 15, 2015, the individual officially separated from the FDIC and removed the portable storage device from FDIC premises.[5] Eight days later, the FDIC became aware of the incident and on November 2, 2015, referred the matter to the OIG.[6] The FDIC worked to recover the device and ultimately took possession of the device on December 8, 2015.[7]

---

[1] Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 8, 2016) [hereinafter Letter, Apr. 8, 2016].
[2] Letter from Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., to Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. (Feb. 26, 2016) [hereinafter Letter, Feb. 26, 2016].
[3] *Id.*; Letter, Apr. 8, 2016, *supra* note 1.
[4] Letter, Feb. 26, 2016, *supra* note 2.
[5] *Id.*
[6] *Id.*
[7] *Id.*

This security incident is particularly troublesome given that the FDIC did not ultimately recover the portable storage device from the former employee until nearly two months after the device was removed from FDIC premises.[8] Given the severity of the breach, compromising over 10,000 individuals' sensitive information, the nearly two-month time frame the FDIC required to recover the device raises serious questions about the FDIC's cybersecurity posture and preparedness to appropriately minimize damage in the aftermath of a breach.

Further, according to information obtained by the Committee, the FDIC did not report the incident to Congress as mandated by FISMA for "major" security incidents until prompted to do so by the FDIC OIG. Over four months after the breach, the FDIC wrote to Congress on February 26, 2016, to inform the appropriate congressional entities of the incident, opting to report the breach only after the OIG informed the FDIC that the incident met the Office of Management and Budget's guidelines for classifying an incident as a "major" security breach.[9] The FDIC's apparent hesitation to inform Congress of the security incident not only raises concerns about the agency's willingness to be transparent and forthcoming with Congress, but raises further questions about whether additional information stored in FDIC systems has been compromised without being brought to the attention of Congress, according to federal statutory requirements.

To assist in the Committee's oversight of the FDIC's response to the October 2015 security incident, please be prepared to discuss the incident with Committee staff during the scheduled briefing. Please also provide the following documents and information as soon as possible, but by no later than noon on May 4, 2016. Unless otherwise noted, please provide the requested information for the time frame October 1, 2015, to the present:

1. All documents and communications referring or relating to the October 2015 security incident, including all communications with the FDIC OIG.

2. A detailed description of the position, grade, and duty location of the former FDIC employee responsible for the breach.

3. A detailed description of the sensitive information copied onto the former FDIC employee's portable storage device.

4. All documents and communications referring or relating to the Office of Management and Budget Memorandum, M-16-03.

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.

---

[8] *Id.*

[9] Memorandum from Shaun Donovan, Dir., Office of Management & Budget to Heads of Executive Departments & Agencies, *Fiscal Year 2015-2016 Guidance on Federal Information Security & Privacy Management Requirements* (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf (last visited Apr. 20, 2016).

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 Lamar Echols or Caroline Ingram at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

Enclosure

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 October 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.