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

October 21, 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 cybersecurity events at the Federal Deposit Insurance Corporation (FDIC) and is in receipt of a notification from you about an additional breach.[1] According to information obtained by the Committee, FDIC personnel initially detected the breach as early as August 9, 2016.[2] This breach involved the compromise of over 400 FDIC employees' documents, including 27 Office of Inspector General (OIG) field agents due to improper permissions set for the agency's "Search+" tool.[3] Due to these permissions deficiencies, all FDIC employees and contractors were able to view all of these individuals' materials housed in their "My Documents" folder on their work computers, including Suspicious Activity Reports, Grand Jury materials, ongoing OIG investigative materials, and OIG deliberative materials.[4] Despite the gravity of this incident and your own testimony that the FDIC would ensure that cybersecurity incidents are reported to Congress in a timely manner,[5] the Committee is concerned that the FDIC's Data Breach Management Team (DBMT) chose not to classify this incident as major.[6] While it is not the Committee's objective to embarrass the FDIC, this recent incident, coupled with the agency's slow-moving response, raises significant concerns about confusion at the FDIC on how to manage cybersecurity incidents, as well as a lack of leadership within the agency on cybersecurity issues.

---

[1] *See, e.g.*, Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 8, 2016); Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 20, 2016); Letter from Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., to Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. (Oct.19, 2016) [hereinafter Letter, Oct. 19, 2016].
[2] *See* FDIC Incident Risk Analysis (IRA) Template, CSIRT INC #228274, at 1 [hereinafter IRA #228274].
[3] *Id.* at 2–3.
[4] *Id.*; Phone Call with FDIC Leg. Affairs Staff & H. Comm. on Science, Space, & Tech. Staff (Sept. 27, 2016).
[5] H. Comm. on Science, Space, & Tech., *Hearing on Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?*, 114th Cong. (Jul. 14, 2016), at 90 [hereinafter Hearing, Jul. 14, 2016].
[6] Phone Call with FDIC Leg. Affairs Staff & H. Comm. on Science, Space, & Tech. Staff (Oct. 13, 2016) [hereinafter Phone Call, Oct. 13, 2016].

The FDIC's October 19, 2016, notification to the Committee states that the FDIC did not find "evidence of unauthorized access" to the files left vulnerable by the breach, contributing to the agency's decision not to classify the incident as major.[7] The Committee understands, however, that your staff may not have in fact conducted a thorough investigation to search for evidence of unauthorized access. Instead, your notification to the Committee merely states without detail that the breach involved OIG staff and that, in total, over ten thousand of folders, "which **may** have contained PII or other sensitive information," were subject to the breach.[8]

According to preliminary determinations made by the FDIC during its attempt to remediate the faulty permissions, there were at least 11,000 open shares of the compromised material.[9] Despite the FDIC's ability to track the number of open shares, the FDIC is unable to track or identify personnel who may have accessed the compromised material.[10] The Committee understands that because of the amount of unknown information associated with the breach, such as the FDIC's inability to track whether personnel accessed the compromised information, and because the breach was internal to the FDIC, that the DBMT opted not to classify the breach as major, therefore not triggering a formal notification to Congress. Instead, over two months after the breach was initially detected and after my staff raised concerns about the breach, Chief Information Officer (CIO) Larry Gross opted to report the incident "out of an abundance of caution."[11]

Given the Committee's extensive investigation into the FDIC's management of cybersecurity breaches and your own testimony under oath that the agency would be responsive to the Committee in reporting breaches,[12] the FDIC's decision to delay reporting this breach to Congress raises significant questions about why the agency would choose not to be forthcoming when it initially learned about the incident. The Committee understands that the FDIC learned about the breach on August 9, 2016,[13] over two months ago, yet did not provide any information to the Committee until my staff reached out to your staff, following our independent receipt of information about the incident. Only after the Committee prompted your staff to provide information about the breach, did the Committee learn additional details about the incident. This chronology indicates that the FDIC never intended to inform Congress of the incident. Unfortunately, this is not the first time the FDIC has decided to conceal a breach from Congress or has failed to report a breach to Congress in a timely manner.[14]

The breadth of this incident, including the compromise of OIG field agents' investigative and deliberative materials, should have warranted a notification to the Committee as soon as the FDIC was aware of the incident, especially given the Committee's keen interest in this topic and

---

[7] Letter, Oct. 19, 2016, *supra* note 1.
[8] *Id.*
[9] *Id.* at 3.
[10] *Id.* at 2–3.
[11] Phone Call, Oct. 13, 2016, *supra* note 6.
[12] Hearing, Jul. 14, 2016, *supra* note 5.
[13] IRA #228274, *supra* note 2.
[14] *See generally* H. Comm. on Science, Space, & Tech., *Hearing on FDIC Data Breaches: Can Americans Trust That Their Private Banking Information is Secure?*, 114th Cong. (May 12, 2016).

its ongoing investigation. Further, the OIG released a report over three months ago with recommendations concerning the very categories of information left vulnerable by this breach. Following the OIG's July 2016, report on a cybersecurity breach involving the compromise of Suspicious Activity Reports,[15] your staff informed my staff that the agency would report any and all incidents as major that involve Suspicious Activity Reports.[16] The delay in reporting this incident, however, raises questions about whether your staff's commitments are being followed in good faith by CIO Larry Gross.

The FDIC's lackluster response to cybersecurity incidents, evidenced by its response thus far to the "Search+" breach, raises significant questions about the FDIC's cybersecurity posture as a whole under your leadership, as well as your testimony before the Committee during its July 14, 2016, hearing. Specifically, during that hearing, you testified that you would ensure that incidents are reported in a timely manner.[17] You stated:

> Rep. Westerman: What kind of steps are you taking to make sure this doesn't happen again?
>
> Mr. Gruenberg: In addition to as a threshold adopting the application of the guidance consistent with the IG's approach, **we're incorporating it in policies and procedures to ensure that any incidents like this are reported in a timely way going forward.**
>
> Rep. Westerman: And what would you say your confidence level is that if something like this were to happen again that it would be reported without the IG having to get involved?
>
> Mr. Gruenberg: **I think at this point I have a pretty high confidence level.**[18]

Your commitment to report incidents in a timely manner to the Committee, however, has *not* been supported by your staff's actions, including those of your CIO Larry Gross. Instead, the Committee has faced reticence time and again from your staff from being forthcoming with the Committee in reporting incidents, opting instead to shield incidents from congressional scrutiny. As you know, the Committee has been receptive to hearing the FDIC's point of view of its response cybersecurity incidents. Given the ever-increasing number of breaches that have occurred at the FDIC, however, which have not been formally reported to the Committee, the Committee is concerned that the FDIC is taking advantage of the Committee's goodwill.

---

[15] *See* FDIC Inspector Gen., *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (Jul. 2016) (AUD-16-004), *available at* https://www.fdicig.gov/reports16/16-004AUD.pdf (last visited Oct. 21, 2016).
[16] Meeting with FDIC Leg. Affairs Staff & H. Comm. on Science, Space, & Tech. Staff (Aug. 10, 2016).
[17] Hearing, Jul. 14, 2016, *supra* note 5 (question and answer by Rep. Westerman).
[18] *Id.* (emphasis added).

As Chairman of the FDIC, the Committee expects you to follow through on your commitments made under oath to the Committee to enact substantive changes to the cybersecurity culture at the FDIC to ensure incidents are reported timely to Congress. Please provide a detailed explanation of specific actions you will immediately take to demonstrate your good faith in fulfilling your testimony. Specifically, please explain what measures you plan to implement to ensure the timely reporting of incidents, including the implementation of policies and procedures to ensure breaches are analyzed appropriately, according to Office of Management and Budget guidance, and reported expeditiously to Congress. Please provide a response no later than noon on October 28, 2016.

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.

When providing responses to the Committee, please deliver responses 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 responses in electronic format.

If you have any questions about this letter, please contact Drew Colliatie or Caroline Ingram with the Committee staff at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman
House Committee on Science,
Space, and Technology

Barry Loudermilk
Chairman
Subcommittee on Oversight
House Committee on
Science, Space, and
Technology

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member, U.S. House Committee on Science, Space, and Technology

The Honorable Don Beyer, Ranking Member, Subcommittee on Oversight, U.S. House Committee on Science, Space, and Technology