

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 19, 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 appreciates the testimony presented by Lawrence Gross, the Federal Deposit Insurance Corporation's (FDIC) Chief Information Officer and Chief Privacy Officer, on May 12, 2016, at a hearing entitled "FDIC Data Breaches: Can Americans Trust that Their Private Banking Information is Secure?" The hearing examined recent cybersecurity breaches that compromised nearly 160,000 individuals' personally identifiable information. At the hearing, Mr. Gross attempted to address the concerns of Committee Members regarding FDIC's lackluster response to the Committee's document requests, whether the data breaches were properly reported to Congress, and what steps Mr. Gross is taking to remedy the recent failures by FDIC to prevent sensitive data from improperly leaving the agency. The Committee is concerned because it appears there are several instances where Mr. Gross' responses to questions posed by Members were false and misleading. Prior to further investigative action by the Committee, we invite you to review Mr. Gross' testimony and provide further details. Should it be necessary to clarify or amend Mr. Gross' testimony, we request that you do so as quickly as possible.

Mr. Gross' Testimony Relating to FDIC's Failure to Provide a Full & Complete Response to the Committee

One of the topics at the May 12, hearing was FDIC's failure to provide a complete response to the Committee's letters dated April 8, 2016,¹ and April 20, 2016.² Your staff confirmed to Committee staff during a telephone call on or about May 6, 2016, that FDIC had provided all responsive documents to both of the Committee's letters. Suspecting that FDIC had withheld certain documents from the Committee, we separately wrote the FDIC Office of Inspector General (OIG) on May 10, 2016, requesting the documents withheld by the agency.³

¹ Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 8, 2016) [hereinafter Letter, Apr. 8, 2016].

² Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (Apr. 20, 2016) [hereinafter Letter, Apr. 20, 2016].

³ Letter from Hon. Lamar Smith, Chairman & Barry Loudermilk, Subcommittee Chairman, H. Comm. on Science, Space, & Tech., to Fred W. Gibson, Acting Inspector General, Fed. Deposit Insurance Corporation. (May 10, 2016) [hereinafter Letter, May 10, 2016].

The next day, OIG provided the Committee with substantially more responsive documents and information than the FDIC had previously produced. This demonstrates a lack of cooperation on the part of FDIC and may in fact be obstruction of the Committee's investigation.

At the May 12 hearing, Oversight Subcommittee Chairman Barry Loudermilk asked why the FDIC OIG was able to provide substantially more documents than the agency despite the Committee requesting the same information from the agency.⁴ Mr. Gross had the following exchange with Chairman Loudermilk:

Rep. Loudermilk: Okay. Thank you. Mr. Gross, what I have here is-- this is the stack of documents that the FDIC provided to the Committee in response to our inquiry. This stack of documents, however--I may need a forklift. This stack of documents was provided to the Committee by the Inspector General's Office. Why were these documents not provided to the Committee by the FDIC?

Mr. Gross: I had an opportunity to review the material provided by the IG, and in reviewing that material, a lot of it is duplicative, so the material that you received from us with the incident response forms that are in there, it includes information that has been duplicated in the IG's response. The incident response forms provide a summary of the incident, and it's—it may in fact provide a more comprehensive review of each of the incidents more so than what's in the documents. I did note that there were several copies of what we call our Data Breach Management Guide that was included in the material provided by the Inspector General, and there were multiple copies of that. That document is still currently being developed and in review.⁵

[...]

Rep. Loudermilk: Okay. Okay. But you did say that you had reviewed the materials—

Mr. Gross: I did—

Rep. Loudermilk: --provided—

⁴ H. Comm. on Science, Space, & Tech., *FDIC Data Breaches: Can Americans Trust that Their Private Banking Information is Secure?*, 114th Cong. (May 12, 2016) [hereinafter FDIC Hearing, May 12, 2016].

⁵ *Id.*

Mr. Gross: I did a cursory review.⁶

Despite testifying that Mr. Gross had reviewed the materials provided by the OIG and stating that “a lot of it is duplicative,” and even giving specific examples of documents he found to be duplicative, Mr. Gross later changed the characterization of his review. When Chairman Loudermilk asked about e-mails withheld from the Committee by FDIC, Mr. Gross shifted his story to say that he had only done a “cursory review” of the materials.⁷ **Further, Mr. Gross’ contention that the documents provided by OIG are duplicative is not accurate.** The agency only provided the Committee with 88 pages of documents responsive to the Committee’s April 20 letter while the OIG provided 883 pages of responsive documents. It appears that Mr. Gross only wanted to provide the Committee with testimony that supported his narrative and was prepared to only discuss examples that were cherry picked from the OIG’s document production.

Chairman Loudermilk also raised concerns about FDIC’s apparent attempts to limit the scope of the Committee’s document request. Mr. Gross had the following exchange with Chairman Loudermilk:

Rep. Loudermilk: To your knowledge, was anyone in your office or the legal division directed to limit the response to the Committee's request?

Mr. Gross: I'm not aware of anyone making such a statement or providing any such direction.⁸

According to information obtained by the Committee, officials in FDIC’s legal department intentionally withheld documents responsive to the Committee’s request by limiting the scope. In fact, it appears that officials in FDIC’s legal department tasked with scoping the document request reached out to Mr. Gross’ office with their proposal to limit the universe of responsive documents. Mr. Gross apparently agreed with the legal department’s scoping of the request given that the documents received by the Committee were only a fraction of the universe of responsive documents. Mr. Gross’ unequivocal statement that he was “not aware of any” documents being withheld from the Committee directly contradicts the Committee’s understanding of FDIC’s document production process.

During the hearing, Chairman Loudermilk presented Mr. Gross with an e-mail specifically relating FDIC’s duty under FISMA to report the Florida data breach incident to Congress – an e-mail clearly responsive to the Committee’s request dated April 20 – yet, withheld from production to the Committee by the FDIC.⁹ Mr. Loudermilk questioned Mr.

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ See E-mail from Christopher J. Farrow, to Lawrence Gross & Richard Lowe (Nov. 30, 2015, 6:33 p.m.).

Gross about why the agency withheld the document.¹⁰ In response, Mr. Gross stated that the e-mail was summarized in materials provided to the Committee.¹¹ Chairman Loudermilk stated:

Rep. Loudermilk: But, sir, did the Committee's request ask for summaries or did it ask for the documents? I believe our request was for all documents, not summaries of documents, but documents.

Mr. Gross: Sir, I believe our response to the Committee's request was comprehensive. We made an active effort to provide a comprehensive response to this committee.

[...]

Rep. Loudermilk: But, sir, you are the addressee on the email with this document, so clearly you did have this document. And it would have been your responsibility to provide this in response to our request for all documents.

Mr. Gross: I believe that this would have been included in the incident response because this document speaks to what's summarized in the incident report.¹²

Despite the Committee's request for "all documents and communications referring or relating to the October 2015 security incident,"¹³ the agency chose to withhold materials, including the e-mail presented to Mr. Gross at the hearing, from production to the Committee.

Although Mr. Gross asserted that responsive documents were "summarized" in the document production,¹⁴ the Committee's investigation found that his assertion is inaccurate. The referenced e-mail is not described with particularity nor is it summarized in the FDIC's document production. Regrettably, as of the date of this letter, the agency continues to withhold responsive documents from the Committee, raising serious questions about whether the FDIC is attempting to conceal potentially incriminating information.

¹⁰ FDIC Hearing, May 12, 2016, *supra* note 4.

¹¹ *Id.*

¹² *Id.*

¹³ Letter, Apr. 20, 2016, *supra* note 2.

¹⁴ FDIC Hearing, May 12, 2016, *supra* note 4.

FDIC's Misleading Characterization of the October 2015 Data Breach in Florida

Additionally, Mr. Gross and individuals briefing Committee staff on April 21, 2016, misled the Committee regarding the circumstances of the Florida breach. At the hearing, Mr. Gross testified about the computer proficiency of the FDIC employees involved in the data breaches, including the October 2015 Florida data breach where the employee refused to return the portable storage device to the FDIC for nearly three months. According to Mr. Gross:

Mr. Gross: The individuals involved in these incidents were not computer proficient. We have policies in place that will allow the FDIC IT staff to assist you when you're departing the organization to copy down things that you may have collected over your long tenure with the agency, specifically, photographs or your personal resume. The fact that they were not computer proficient, if you go in and you don't copy the material and do it as a targeted copying of that information, you could in fact inadvertently copy the entire hard drive. So if you insert and you do the copy and not being proficient in the technology, you may take more data than what you intended.

According to information obtained by the Committee, Mr. Gross was aware that the FDIC employee involved in the Florida incident was indeed computer proficient. Based on the Committee's investigation, the Committee determined the employee holds two master's degrees, including one in Information Technology Management. Moreover, according to the university website describing the Master's in Information Technology program where the employee received her degree, "the master's degree in information technology management focuses on emerging technologies and the management of both IT and people engaged in **computer technology enterprises**."¹⁵ Mr. Gross' claim that the employee in question was not computer proficient raises serious questions regarding whether his testimony was intentionally misleading.

On April 21, 2016, FDIC briefed Committee staff on the October 2015 Florida data breach. During that briefing, FDIC staff relayed to Committee staff that the former FDIC employee committing the breach was non-adversarial, was simply trying to download family photos, was going through a divorce, and experiencing personal problems in her life.¹⁶ In reality, the Committee learned that this individual denied owning a portable storage device, claimed she would never do such a thing, and ultimately hired an attorney to engage in a protracted negotiation of the return of the portable storage device and the affidavit she signed.

¹⁵ Webster University, *Master's in Information Technology Management*, available at <http://www.webster.edu/business-and-technology/academics/information-technology-management.html> (last visited May 19, 2016).

¹⁶ Briefing by FDIC Staff, April 21, 2016.

Additionally, during the hearing, Mr. Gross continued to perpetuate this misleading story. He testified that in all of the recent breaches reported to Congress, FDIC employees inadvertently copied the data to portable storage devices, including the employee in the Florida case who held a master's degree in information technology. When describing the FDIC employee in the Florida incident, Mr. Gross testified:

Mr. Gross: I believe she, on the surface, was telling the truth, but I don't think she really understood that she had taken--one, I think she realized she took her personal data. I don't believe she realized she took FDIC-specific data. And in each of these cases, these are all referred to the IG's office. Every one of these cases we had asked the IG if they were going to investigate the case. The response we received is that there was no criminal activity; therefore, it did not warrant any further action on their part.¹⁷

It appears that Mr. Gross is glossing over the fact that the employee made false statements to the FDIC when the agency attempted to recover the portable storage device.¹⁸ Indeed, the employee said she "would never do such a thing." Moreover, considering the employee holds a master's degree in information technology, it is troubling that she told the agency that she did not own an external hard drive or even know what an external hard drive is. Serious questions are raised when an FDIC employee holding a master's degree in technology denies even knowing about basic computer technology and Mr. Gross, the CIO, believes the story. Just as troubling, Mr. Gross takes no issues with the fact the FDIC employee was less than forthcoming with the agency and withheld important data from the portable storage device from FDIC for nearly three months.

Mr. Gross Intentionally Misled the Committee by Characterizing the Breaches as Low Risk

Further, it appears that Mr. Gross has shifted his view that the data breaches were low risk. Specifically, when asked why credit monitoring had not been offered to the victims of the data breaches, Mr. Gross explained:

Mr. Gross: We evaluated each of the cases and determined because there was low risk of harm that there were no individuals that were affected or impacted adversely as a result of the downloading of the information. **So as a result of the lack of impact to the individuals, it was deemed that credit monitoring was not warranted.** We have in other cases where the information has been taken and we

¹⁷ FDIC Hearing, May 12, 2016, *supra* note 4.

¹⁸ See Letter from Barbara Katron, Senior Counsel, FDIC to Daniel Valdivia, the Valdivia Law Firm (Dec. 2, 2015) [hereinafter Letter, Dec. 2, 2015].

know it was a known adversary or someone with adverse intent where they may break in an employee's car and steal records, we know that that individual had ill intent by breaking in the car. That information, regardless of the number of records that may have been exposed, in those cases we would have offered credit monitoring, as we've done in the past.

While Mr. Gross testified that the lack of impact on the victims resulted in credit monitoring *not* being necessary, he reportedly changed his mind hours after the Committee's hearing. According to the *Washington Post*, FDIC will provide credit monitoring for the victims impacted by FDIC's recent data breaches.¹⁹ While the Committee welcomes Mr. Gross' decision to finally offer credit monitoring to the victims of the data breaches, the decision raises questions about Mr. Gross' prior judgment, including whether Mr. Gross still believes the recent breaches have little impact on the victims.

Steps Taken by the FDIC to Prevent Future Breaches are Worthless and FDIC Continues to Ignore FISMA Requirements to Report to Congress

During Mr. Gross' opening statement, he cited steps the FDIC has taken to remediate the risk of sensitive information being exposed. He specifically stated: "We have already implemented technology to remove the ability of the **majority** of employees to download any data from FDIC systems to portable media."²⁰ **Yet, when asked during the hearing about steps the agency has taken to limit the use of portable storage devices by agency employees, Mr. Gross stated that about 50 percent of employees still have the ability to download data onto portable storage devices.²¹ Even more troublesome, Mr. Gross could not certify that the remedial actions taken could have prevented the breaches.²²** Mr. Gross testified:

Mr. Gross: I believe we've reduced that number down to probably less than 50 percent.

[...]

Rep. Loudermilk: So if you had these 50 percent--let me ask it this way. If the 50 percent you have blocked now was done 6 months ago, would it have prevented these incidents?

¹⁹ See Joe Davidson, *Congress Hits FDIC Cyber Breach that 'Boggles the mind'*, WASH. POST, May 13, 2016, available at <https://www.washingtonpost.com/news/powerpost/wp/2016/05/13/congress-hits-official-called-naive-or-incompetent-over-fdic-cyberbreaches/>.

²⁰ See Statement of Lawrence Gross, Chief Information Officer, Fed. Deposit Insurance Corp. (May 12, 2016), at 5 (emphasis added).

²¹ FDIC Hearing, May 12, 2016, *supra* note 4, at 68–69.

²² *Id.*

Mr. Gross: I can't say that for certain, sir, because these individuals were in various different parts of the organization. And even, as I said, it was an inadvertent download of the data.²³

Further, Mr. Gross' statement regarding an e-mail he received on April 28, 2016 related to reporting data breaches to Congress raises questions. According to the email from Roderick Toms, the Acting Chief Information Security Officer, sent to Mr. Gross, "[w]e were notified of the 10K record count for these incidents on 4/27 so the 7 day reporting requirement will be 5/4." Mr. Gross testified:

Mr. Gross: I don't know if this incident was reported by May 4. I believe it was reported in the recent report where we provided five different incidents to the Congress.

Fred Gibson, FDIC's Acting Inspector General was also asked about the same e-mail. According to Mr. Gibson:

Mr. Gibson: Sir, I think that when the waterfall requirements of 16-03 are triggered, I think that there's an obligation to report in 7 days from the time that the agency has a reasonable basis to believe that a major incident has occurred. That's what the law says.

Despite the fact that Mr. Gross was on notice that he was required to disclose data breaches at FDIC on May 5, 2016, he failed to do so. As Mr. Gibson testified, there is in fact a 7 day obligation to report such an incident. It raises concerns that Mr. Gross is not even aware whether this recent incident was timely reported to Congress in compliance with federal law.

Although the Federal Information Security Modernization Act of 2014 (FISMA) **requires** Executive Branch departments and agencies to report "major" incidents to Congress,²⁴ Mr. Gross explained during the hearing that, in his view, FISMA and the specifically delineated requirements outlined in the Office of Management and Budget (OMB) memorandum for classifying "major" incidents²⁵ provide "some guidance to the agency to consider in making a determination of, one, the significance of an event."²⁶ He went on to testify, however, that the determination on whether an incident is major is still up to the discretion of the agency, including

²³ *Id.* (emphasis added).

²⁴ Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (emphasis added).

²⁵ 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 May 19, 2016).

²⁶ FDIC Hearing, May 12, 2016, *supra* note 4.

a consideration of whether the issues surrounding the incident merit reporting the incident to Congress within seven days.²⁷

Mr. Gross' interpretation of FISMA requirements and OMB guidelines for reporting major incidents to Congress appears to ignore OMB's guidance, which instructs agencies to consider the sensitivity of breach details. With respect to whether to report the Florida incident to Congress, which the FDIC reported over four months after the breach, the agency, including Mr. Gross, apparently thought that the former employee's circumstances in her personal life trumped notifying Congress or any of the victims about the incident. This is despite the fact that over 10,000 individuals' Social Security numbers and customer data were removed from the premises. Mr. Gross and the FDIC's dilatory approach to notifying Congress of major incidents raises serious questions about whether the agency's ability to manage its information technology systems in accordance with the requirements outlined by FISMA and OMB.

Providing false or misleading testimony to Congress is a serious matter. Witnesses who purposely give false or misleading testimony during a congressional hearing may be subject to criminal liability under Section 1001 of Title 18 of the U.S. Code, which prohibits "knowingly and willfully" making materially false statements to Congress. With that in mind, we write to request that Mr. Gross correct the record and to implore him to be truthful with the American public about matters related to FDIC cybersecurity breaches. Please provide further details on each of the matters discussed in this letter as soon as possible, but by no later than noon on May 26, 2016.

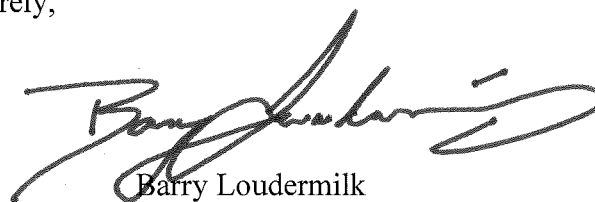
The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology which develops cybersecurity standards and guidelines to support the implementation of and compliance with FISMA as set forth in House Rule X.

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
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

²⁷ *Id.*