



# Special Inquiry Report

## The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches

April 2018

OIG-18-001





**Date:** April 16, 2018

**Memorandum To:** Martin J. Gruenberg  
Chairman

**From:** Jay N. Lerner  
Inspector General

**Subject** | Special Inquiry: *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (OIG Report No. OIG-18-001)

This report presents the results of our Special Inquiry. My Office conducted this review at the request of the former Chairman of the Senate Committee on Banking, Housing, and Urban Affairs. The former Committee Chairman asked that the FDIC Office of Inspector General examine issues at the FDIC related to data security, incident reporting, and policies, as well as representations made by FDIC officials to Congress.

The report contains 13 recommendations to address systemic issues associated with the FDIC's incident response and reporting, and interactions with Congress. We also discuss issues related to certain individuals' performance of their responsibilities during the timeframes under review.

We appreciate the cooperation of all FDIC staff throughout the course of our Special Inquiry.



## Executive Summary

### The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches

---

During late 2015 and early 2016, the Federal Deposit Insurance Corporation (“FDIC”) experienced eight information security incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven of the eight incidents involved Personally Identifiable Information (“PII”), including Social Security Numbers, and thus constituted breaches. In the eighth incident, the departing employee took highly sensitive components of resolution plans submitted by certain large systemically important financial institutions without authorization.

In April and May 2016, the Committee on Science, Space, and Technology of the House of Representatives (“SST Committee”) examined the FDIC’s handling of these incidents, its data security policies, and reporting of the “major incidents.” As part of its investigation, the SST Committee requested pertinent documents from the FDIC about the incidents. The SST Committee held two hearings in May and July 2016 about the incidents at the FDIC and issued an interim report on the matter. During the hearings and in its interim report, as well in correspondence with the FDIC, the SST Committee expressed concerns about the FDIC’s information security program, the accuracy of certain FDIC statements, and the completeness of the FDIC’s document productions.

#### Special Inquiry Purpose and Approach

On June 28, 2016, the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that the FDIC Office of Inspector General (“OIG”) examine issues at the FDIC related to data security, incident reporting, and policies, as well as the representations made by FDIC officials.

The FDIC OIG conducted this Special Inquiry in response to that request. We examined the circumstances surrounding the eight information security incidents. The FDIC initially estimated that the incidents involved sensitive information that included the PII of approximately 200,000 individual bank customers related to approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions. Based on additional analysis, the FDIC later revised the number of affected individuals to 121,633.

Our Special Inquiry report provides the historical context for these incidents and the prior oversight work of the FDIC’s information technology systems, including the OIG’s prior and ongoing work. We also establish the relevant law, guidance, standards, authorities, policies, programs, and procedures applicable to information security incidents and breaches and the incident response program at the FDIC at the time of the incidents.

## Executive Summary

---

Our Special Inquiry report then presents the facts, and our analysis and recommendations relating to the following three areas:

- The FDIC’s Handling of the Information Security Incidents;
- The FDIC’s Reporting and Statements to Congress Regarding the Information Security Incidents; and
- The FDIC’s Document Production to Congress.

The final section of the report contains our conclusions, including systemic and performance issues.

### **The FDIC’s Handling of the Information Security Incidents**

At the outset, we found that the FDIC had not taken sufficient steps to ensure that it had a comprehensive incident response program and plan for information security incidents and breaches. Importantly, it did not have timely legal guidance on the reporting requirements pursuant to Federal Information Security Modernization Act of 2014 (“FISMA 2014”) and guidance from the Office of Management and Budget implementing the FISMA 2014 statute. Further, the FDIC did not ensure that risk assessments and decisions associated with the incidents were clearly documented. Absent such documentation, the FDIC could not ensure consistent treatment of incidents, and it did not have precedent to evaluate potential future misconduct. In addition, there was not sufficient information for the FDIC or an oversight body to conduct proper supervision of the program.

We also determined that the manner in which the FDIC prepared the former employees’ post-employment statements did not fully protect the FDIC’s interests. In addition, the FDIC did not fully consider the range of impacts on bank customers whose information had been compromised or consider customer notification as a separate decision from whether it would provide credit monitoring services. As a result, the FDIC delayed notifying consumers and thus precluded them from taking proactive steps to protect themselves. The FDIC did not notify consumers for at least 8 months after the FDIC first discovered the incidents, and in some cases, the FDIC did not notify consumers until more than a year after.

### **The FDIC’s Reporting and Statements to Congress Regarding Information Security Incidents**

The FDIC should have been more timely and precise in its reporting of the information security incidents. For example, the FDIC’s notifications to Congress that “major incidents” had occurred were not timely. Even after it became apparent that incidents had potentially affected more than 10,000 individuals or records, the FDIC delayed reporting the incidents. As

## Executive Summary

---

a result, the FDIC did not report the incidents to Congress within the 7-day statutory requirement.

In the case of one incident, the FDIC did not sufficiently convey its seriousness, opting to report the incident in its annual FISMA submission along with other less serious incidents, and omitting the fact that it involved the breach of very sensitive information. Further, with respect to the other seven information security incidents, when reporting those to Congress, the FDIC used broad characterizations and referenced mitigating factors. These characterizations and factors were sometimes inaccurate and imprecise, and tended to diminish the potential risks. Despite several opportunities to clarify or correct the record regarding the nature of the incidents, the FDIC did not provide Congress with accurate and complete information about the incidents.

### The FDIC's Document Production

As the SST Committee was examining the FDIC's handling and reporting of "major incidents," the Committee requested that the FDIC produce relevant documents and information. In that regard, we found that the FDIC did not initially respond to these requests in a complete manner. At first, the FDIC did not impose a legal hold on a number of individuals who had direct and relevant knowledge of the facts, including senior FDIC officials in Information Technology, Legal, and Legislative Affairs, and other key staff involved in responding to the incidents. Therefore, the FDIC could not be sure that these individuals had retained relevant records in their possession. Further, the FDIC did not initially conduct searches of the FDIC's email vault to identify responsive records. During this timeframe, the FDIC should have been clear in its communications with and testimony before the SST Committee regarding its approach and progress in complying with document production requests. Only later when Congress requested that the FDIC specifically preserve all pertinent documents did the FDIC broaden its legal hold, more thoroughly search its records, provide responsive documents from the expanded records search, and engage in discussions with the SST Committee about its process for identifying and providing responsive records.

### Conclusions and Recommendations

Our work revealed certain systemic weaknesses that hindered the FDIC's ability to handle multiple information security incidents and breaches efficiently and effectively; contributed to untimely, inaccurate, and imprecise reporting of information to Congress; and led to document productions that did not fully comply with Congressional document requests. We also identified shortcomings in the performance of certain individuals in key leadership positions as

## Executive Summary

---

they handled the incidents and related activities, namely the former Chief Information Officer/Chief Privacy Officer, the Director of the Office of Legislative Affairs, and the former Deputy General Counsel.

Throughout and subsequent to our Special Inquiry, the FDIC took steps to address prior recommendations pertaining to incident and breach response. In addition, we made 13 recommendations in this Special Inquiry report to address the systemic issues associated with the FDIC's incident response and reporting and interactions with Congress. We also requested that the FDIC review the performance issues we identified and advise the OIG of actions taken to address them.

The FDIC concurred with the 13 recommendations in this Special Inquiry report. The FDIC has completed corrective actions for 2 of the recommendations and plans to implement corrective actions to address the remaining 11 between June 2018 and December 2018. The FDIC also agreed to advise the OIG of actions undertaken to address the performance issues.

# Contents

	Page
I. Introduction .....	1
II. Historical Context for Information Security Incidents at the FDIC.....	5
III. Standards Governing the FDIC’s Information Technology Security and Handling of Information Security Incidents and Breaches .....	17
A. Key Leadership Positions Governing FDIC Information Technology .....	17
B. Statutes and Guidance Governing Incident and Breach Response and Reporting .....	20
C. The FDIC’s Information Security and Privacy Programs.....	24
D. The FDIC’s Policies and Procedures in 2015 and 2016.....	26
IV. Factual Circumstances of the Handling of Information Security Incidents and Breaches at the FDIC.....	35
A. The New York Incident .....	36
B. The Florida Incident .....	37
C. Incident A .....	41
D. Incident B .....	43
E. Incident C .....	45
F. Incident D .....	49
G. Incident E.....	51
H. Incident F.....	53
V. OIG Findings and Analysis Regarding the FDIC’s Handling of Information Security Incidents and Breaches.....	55
A. The FDIC Did Not Have Implementation Guidance and Procedures to Meet Statutory FISMA 2014 Deadlines .....	55
B. The FDIC Did Not Adhere to Existing Policies in Responding to the Florida Incident and That Approach Carried Over to Subsequent Incidents .....	60
C. The FDIC Placed Undue Reliance on Post-Employment Written Statements from Former Employees .....	64
D. The FDIC’s Notifications to Consumers Were Not Timely .....	66
E. Designating the CIO and SAOP/CPO Roles Within the Same Position Warrants Further Evaluation.....	68
F. The FDIC Did Not Timely Notify the Financial Crimes Enforcement Network .....	70
G. The FDIC Lacked Procedures and Resources to Promptly Review Information Generated by the Data Loss Prevention Tool .....	71



# Contents

	Page
H. Recommendations .....	73
VI. The FDIC’s Reporting and Statements Regarding the Information Security Incidents and Breaches.....	75
A. Initial Notifications to Congress Under FISMA 2014.....	75
B. Subsequent FDIC Interactions with Congress Regarding the Information Security Incidents and Breaches .....	79
VII. OIG Findings and Analysis Regarding the FDIC’s Reporting and Statements.....	85
A. The FDIC’s Notifications to Congress under FISMA 2014 Were Not Timely .....	85
B. The FDIC’s Characterization of the New York Incident Did Not Convey Its Seriousness ..	87
C. The FDIC’s Statements Regarding the Breaches Included Characterizations That Were Overly Broad and Did Not Convey Potential Risks .....	89
D. Subsequent FDIC Statements Repeated Earlier Assertions and Did Not Correct the Prior Record .....	94
E. The FDIC’s Statements Regarding Customer Notifications Overstated Progress .....	96
F. Recommendations .....	96
VIII. The FDIC’s Document Productions to Congress.....	97
A. The SST Committee’s Initial Request Regarding Incident F and the FDIC’s Response (April 8 and 22, 2016).....	97
B. The SST Committee’s Request Regarding the Florida Incident and the FDIC’s Response (April 20 and May 4, 2016) .....	100
C. Telephone Call between FDIC Office of Legislative Affairs and SST Committee Staff (May 6, 2016) .....	102
D. SST Committee’s Subcommittee on Oversight Hearing (May 12, 2016) .....	104
E. SST Committee Letter to the FDIC Chairman (May 24, 2016) and the FDIC’s Subsequent Responses .....	104
IX. OIG Findings and Analysis Relating to the FDIC’s Document Production .....	105
A. The FDIC’s Initial Productions Were Not Complete and Did Not Comply with SST Committee Instructions .....	105
B. The FDIC Did Not Initially Take Sufficient Steps to Identify Responsive Documents.....	106
C. The FDIC Lacked Specific Policies and Procedures for Responding to Congressional Document Requests.....	107
D. Then-CIO Gross’ Statements about the FDIC’s Document Productions Were Not Accurate and the FDIC Did Not Correct the Record.....	107

# Contents

	Page
E. Recommendations .....	109
X. Conclusion .....	110
XI. Comments from the FDIC and Former FDIC Officials.....	113

## Appendices:

I. Objective, Scope and Methodology.....	114
II. The Senate Banking Committee’s June 28, 2016 Letter to the OIG and the OIG’s July 29, 2016 Response. ....	117
III. Pre-Exit Clearance Record for Employees .....	121
IV. Data Questionnaire for Departing/Transferring Employees/Contractors.....	123
V. Former Employees’ Statements.....	125
VI. Letters Reporting Seven “Major Incidents” to the SST Committee.....	135
VII. The SST Committee’s April 8, 2016 Letter to the FDIC and the FDIC’s April 22, 2016 Response.....	144
VIII. The SST Committee’s April 20, 2016 Letter to the FDIC and the FDIC’s May 4, 2016 Response. ....	153
IX. The SST Committee’s May 19, 2016 Letter to the FDIC and the FDIC’s May 25, 2016 Response. ....	162
X. The SST Committee’s May 27, 2016 Letter to the FDIC and the FDIC’s June 20, 2016 Response.....	173
XI. The SST Committee’s August 1, 2016 Letter to the FDIC and the FDIC’s August 25, 2016 Response. ....	181
XII. The FDIC’s September 23, 2016 Letter to the SST Committee.....	193
XIII. The SST Committee’s May 10, 2016 Letter to the OIG and the OIG’s May 11, 2016 Response. ....	201
XIV. The SST Committee’s May 24, 2016 Letter to the FDIC and the FDIC’s June 7, 2016 Response. ....	205
XV. Glossary of Terms. ....	216
XVI. Acronyms and Abbreviations.....	220
XVII. The FDIC’s Response to This Report .....	222

# Contents

	Page
XVIII. The FDIC’s Planned Corrective Actions and Associated Timeframes .....	231

## Table:

1. Key Dates Associated with the Eight Data Breaches .....	35
------------------------------------------------------------	----

## Figures:

1. FDIC IT Governance Structure.....	25
2. FDIC Breach Response Life Cycle .....	27
3. Five Factors of Risk Assessment Methodology.....	29
4. Timeline for New York Incident .....	36
5. Timeline for Florida Incident.....	37
6. Timeline for Incident A.....	41
7. Timeline Incident B .....	43
8. Timeline for Incident C.....	45
9. Timeline for Incident D .....	49
10. Timeline for Incident E.....	51
11. Timeline for Incident F.....	53
12. Security Violations Detected.....	72

## I. Introduction

According to the United States Computer Emergency Readiness Team<sup>1</sup> (“US-CERT”), federal government agencies reported more than 50,000 security incidents involving personally identifiable information (“PII”) to US-CERT from 2014 through 2016.<sup>2</sup> Such incidents may include insider threats like employees or contractor personnel within an organization who compromise information and systems by mistake or through intentional acts with improper motives; or outside threats such as hackers, criminals, foreign actors, terrorists, or other nefarious groups who execute cyber-based attacks. These threats underscore the criticality of establishing an effective, enterprise-wide information security program.

As a bank regulator, the Federal Deposit Insurance Corporation (“FDIC”) collects and maintains a significant volume of highly sensitive information, including PII. PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security Number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. The FDIC maintains PII in such forms as bank customer information about personal finances; personnel information about bank employees; and investigative information about ongoing enforcement efforts, including Suspicious Activity Reports.<sup>3</sup>

The FDIC also maintains business proprietary information that is sensitive, such as a bank’s internal operations regarding counterparties, vendors, suppliers, and contractors. Further, in the case of certain large financial institutions—known as “Systemically Important Financial Institutions” (“SIFI”)—the FDIC collects and stores documents that demonstrate how the institutions would dissolve themselves in a timely and orderly manner in the event of serious financial distress or failure. The FDIC must safeguard this information from unauthorized access or disclosure that could lead to harm to the agency or a financial institution, identity theft or fraud against individual consumers, or potential legal liability or exposure for the FDIC and banks.

---

<sup>1</sup> Certain terms that are underlined when first used in this report are defined in Appendix XV, Glossary of Terms.

<sup>2</sup> US-CERT is an organization within the Department of Homeland Security that assists federal civilian agencies with their incident handling efforts. The Federal Information Security Modernization Act of 2014 requires federal agencies to report security incidents to US-CERT, which analyzes the information to identify trends and indicators of attack across the federal government.

<sup>3</sup> We discuss the content and use of Suspicious Activity Reports on page 10 of this Special Inquiry report.

Guidance from the Office of Management and Budget (“OMB”) in 2017 (“OMB Memorandum M-17-12”)<sup>4</sup> describes the gravity of breaches:

Over the past decade, discussions about the risk of harm to individuals resulting from a breach have generally focused on financial- or credit-related identity theft such as using a stolen credit card number, opening a new bank account, or applying for credit in another person’s name. Today, however, malicious actors use stolen PII, modern technology, and forged identity documents to:

- seek employment;
- travel across international borders;
- obtain prescription drugs;
- receive medical treatment;
- claim benefits;
- file false tax returns; and
- aid in other criminal activities.

Additionally, identity theft – the harm most often associated with a breach – remains a significant problem in the United States.

Identity theft represented 16 percent (490,220) of the over 3 million complaints received by the Federal Trade Commission (“FTC”) in 2015. In 2014, the Department of Justice reported that 17.6 million individuals, or 7 percent of all U.S. residents age 16 or older, were victims of one or more occurrences of identity theft. Moreover, new types of identity theft are emerging, such as synthetic identity theft, which occurs when a malicious actor constructs a new identity using a composite of multiple individuals’ legitimate information along with fabricated information.

As the ways in which criminals can exploit PII have evolved, so too have the ensuing types of harm to potentially affected individuals. Identity theft can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and, in rare cases, risk to personal safety.

Because of the harm associated with information security incidents or breaches, a statute was enacted that requires federal agencies to develop programs to prevent, respond, and

#### What is a breach?

OMB defines the term “breach” as a type of security incident that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. A breach can be inadvertent, such as a loss of hard copy documents or portable electronic storage media, or deliberate, such as a successful cyber-based attack by a hacker, criminal, or other adversary.

---

<sup>4</sup> OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, dated January 3, 2017.

report such incidents. The Federal Information Security Management Act of 2002 (“FISMA”) statute,<sup>5</sup> as amended in 2014, requires that certain serious incidents, known as “major incidents,” must be reported to Congress within 7 days.

Historically, the FDIC has faced a number of information security incidents. In August 2011, the FDIC began to experience a sophisticated, targeted attack on its network known as an Advanced Persistent Threat (“APT”). An APT may occur when an entity gains unauthorized access to a computer network, escalates its privileges, and develops an ongoing presence within the network to compromise the network data and component level security. The attacker behind the APT penetrated more than 90 workstations or servers within the FDIC’s network over a significant period of time, including computers used by the former Chairman and other senior FDIC officials. The attacker further gained unauthorized access to a significant quantity of sensitive data.

In response to the APT, the FDIC modified its security governance structure by separating the positions of Chief Information Officer (“CIO”) and Director of the Division of Information Technology (“DIT”) and moving the information security and privacy functions directly under the CIO. The FDIC also established a senior-level committee for assessing cyber-security threats and strengthened procedures to address future information technology (“IT”) security incidents. In addition, the FDIC hired a consulting firm, which made 23 recommendations primarily addressing the areas of authentication controls, administrative privileges, firewall configurations, and audit and logging settings. According to FDIC records, as of December 1, 2017, 18 of these recommendations were implemented, 3 were already in place before the consulting firm’s report was issued, and 2 were deemed not feasible due to the negative impact on the FDIC business environment. The FDIC believed that it had mitigating controls in place for the two recommendations deemed not feasible.

In late 2015 and 2016, eight incidents were detected as departing employees improperly took sensitive information shortly before leaving the FDIC. Based on information gathered during the incident response and remediation process, the FDIC determined that seven of the eight incidents were breaches and initially estimated that this sensitive information included the PII of approximately 200,000 individual bank customers related to approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions. Based on additional analysis, the FDIC later revised the number of affected individuals to 121,633. The eighth incident involved sensitive financial institution

---

<sup>5</sup> Public Law 107-347, the E-Government Act of 2002, Title III, Section 301, enacted on December 17, 2002.

information but did not involve PII; therefore, by OMB definition, the incident was not considered to be a “breach.”

In early 2016, the Committee on Science, Space, and Technology of the U.S. House of Representatives (“SST Committee”) examined the FDIC’s handling of these “major incidents,” its data security policies, and reporting of these “major incidents.” As part of its investigation, the SST Committee requested documents from the FDIC about the incidents, its reporting, and its policies for handling such incidents. The SST Committee held two hearings in May and July 2016 about the incidents and issued an interim report on the matter. During the hearings and in its interim report, as well as in correspondence with the FDIC, the SST Committee expressed concerns about the FDIC’s information security program, the accuracy of certain FDIC statements, and the completeness of the FDIC’s document productions.

On June 28, 2016, the then-Chairman of the U.S. Senate Committee on Banking, Housing, and Urban Affairs (“Senate Banking Committee”) requested that the FDIC Office of Inspector General (“OIG”) examine institutional issues at the FDIC related to data security, incident reporting, and policies governing departing employees’ access to sensitive information, as well as the representations made by FDIC officials. On July 29, 2016, we confirmed that we would conduct a Special Inquiry into the matter. (See Appendix II for the Senate Banking Committee’s request and the OIG’s response.)

The scope of this Special Inquiry included reviewing the facts surrounding the information security incidents and representations made by the FDIC, examining the FDIC’s initial responsiveness to the requests from the SST Committee for documents, and reviewing its original decision not to report the “major incidents” to Congress. This Special Inquiry also addressed the extent to which the FDIC had developed and implemented certain policies and procedures relevant to the handling and reporting of these incidents.

To conduct our work, we reviewed relevant law, guidance, standards, authorities, policies, programs, and procedures; interviewed 24 current and former FDIC employees; gathered documents from witnesses; performed searches across the FDIC’s email vault; and obtained and reviewed documents associated with incident response activities and interactions with Congress, including all documents that the FDIC produced to the SST Committee. In addition, in September and October 2016, OIG and Financial Crimes Enforcement Network (“FinCEN”) special agents interviewed six former employees who

improperly took information from the FDIC.<sup>6</sup> Further details on our methodology are included in Appendix I to this report.

We organized this Special Inquiry report to initially provide the proper background and context for the results of our work. First, we discuss the scope and breadth of the oversight efforts to examine the FDIC's information systems, and next, we discuss the relevant law, guidance, standards, authorities, policies, programs, and procedures applicable to breaches and the incident response program at the FDIC.

This Special Inquiry report then presents the results regarding:

- The FDIC's Handling of the Information Security Incidents,
- The FDIC's Reporting and Statements to Congress Regarding the Information Security Incidents, and
- The FDIC's Document Production to Congress.

In each section, we discuss the facts developed during the Special Inquiry, which are followed by our analysis and findings, and our recommendations. We also provide copies of pertinent documents, correspondence between the FDIC and Congress, a glossary of terms, and a list of acronyms and abbreviations used in our Special Inquiry report in Appendices III through XVI. We have included the FDIC's response to this report and its planned corrective actions and associated timeframes for completion as Appendices XVII and XVIII.

## **II. Historical Context for Information Security Incidents at the FDIC**

In recent years, the FDIC OIG has increased its focus on the FDIC's IT systems, consistent with the elevated risks at the FDIC and in the banking sector. We provide this information as background and context for the information security incidents in late 2015 and 2016, and the FDIC's incident response program.

***Investigation of Computer Incident*** (May 2013).<sup>7</sup> In March 2013, the FDIC OIG received information that raised serious concerns as to how the August 2011 APT was handled and communicated both within and outside the FDIC. Accordingly, the OIG initiated an

---

<sup>6</sup> The Financial Crimes Enforcement Network is a bureau of the Department of the Treasury that aims to "safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."

<sup>7</sup> Due to the sensitivity of information included in this investigation report, the FDIC OIG did not publicly release the report.



investigation to understand the events surrounding the incident. Our investigation found that the FDIC Chairman and other senior FDIC officials were not fully informed about the risks associated with the APT nor the progress and efficacy of mitigation steps. We also reported that the FDIC did not follow its policies and procedures, nor properly notify and report the incident to appropriate federal agencies, financial institutions, private sector service providers, the FDIC OIG, and Government Accountability Office (“GAO”) auditors.

***The FDIC’s Information Security Program*** (November 2013).<sup>8</sup> In our annual FISMA review in 2013, we concluded that the FDIC had established and maintained many information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology (“NIST”) standards and guidelines. Notably, the FDIC had established security policies and procedures in almost all of the security control areas we evaluated. The FDIC also was working to develop a formal concept-of-operations document that describes a corporate-wide approach to information security continuous monitoring.

However, we found that the FDIC needed to implement control improvements to more effectively identify, evaluate, and mitigate risk to the FDIC’s information systems and data. Specifically, the FDIC needed to strengthen its incident response policies and procedures to address sophisticated, cyber-based security incidents and update its corporate information security risk management policy to reflect changes in its risk management processes and governance. The FDIC also needed to better ensure that certain servers and workstations were patched to protect against known vulnerabilities, place greater emphasis on assessing risks associated with the FDIC’s outsourced information systems and services, and perform further analysis to ensure that information systems supporting mission essential functions could be recovered within the timeframes needed to support those functions.

***The FDIC’s Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act*** (July 2014).<sup>9</sup> Our audit report found that the FDIC’s controls for safeguarding sensitive information in resolution plans, often referred to as “living wills,” were not fully consistent with applicable information security requirements, policies, and guidelines. The Dodd–Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank Act”) requires SIFIs to file “living will”-related documents to demonstrate how the institution would dissolve itself in a timely and orderly manner in the event of serious

---

<sup>8</sup> A summary of this report is available at <https://www.fdicog.gov/sites/default/files/publications/14-002AUD.pdf>.

<sup>9</sup> A copy of this report is available at <https://www.fdicog.gov/sites/default/files/publications/14-008AUD.pdf>.

financial distress or failure. These “living wills” contain very sensitive information, including:

- Information about critical vendors, suppliers, and associated agreements that SIFIs maintain;
- A description of the actions that SIFIs would or would not take to support clients and vendors under stress;
- Non-public financial and business data;
- Personal information about employees;
- Location and activities of data centers; and
- A list of critical operations.

Among other things, we recommended that the FDIC update its security policies and procedures for the Office of Complex Financial Institutions (“OCFI”), strengthen access controls, and assess the role and level of resources allocated to OCFI’s internal review and information security functions. Throughout 2013, and prior to the close of the audit in February 2014, the FDIC was taking actions to address our preliminary observations and strengthen security controls over sensitive resolution plan information. These actions significantly improved the state of security over sensitive “living will” information.

Our report made recommendations regarding enhanced controls relating to access management, encryption and authentication, internal control reviews, and personnel suitability. The FDIC implemented our recommendations.<sup>10</sup>

***The FDIC’s Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties*** (March 2015).<sup>11</sup> The FDIC OIG conducted a review of the FDIC’s internal controls to properly identify, secure, and dispose of PII in properties referred to as Owned Real Estate (“ORE”). The FDIC may initially acquire an ORE property because it is on the books and records of a failed financial institution, or through the foreclosure process. The FDIC typically identifies PII in ORE properties through physical site inspections once the properties come into its possession.

---

<sup>10</sup> A recommendation is considered implemented once the OIG determines that the corrective action taken to address the recommendation is sufficient. The status of recommendations we reference throughout this report is as of January 16, 2018. In the case of certain unimplemented recommendations, the proposed corrective action is either being reviewed internally by the FDIC or the OIG. A list of current unimplemented recommendations is available on our website at <https://www.fdicog.gov/unimplemented-recommendations>.

<sup>11</sup> A copy of this report is available at <https://www.fdicog.gov/sites/default/files/publications/15-004AUD.pdf>.

We found that the FDIC established a number of internal controls during the course of our audit that were designed to properly identify, secure, and dispose of PII at ORE properties. For example, the Division of Resolutions and Receiverships (“DRR”) modified its ORE contracts in October 2014 to require that the contractors search for PII during every property site inspection.

Notwithstanding those steps, we determined that the FDIC had found PII at 10 ORE properties we sampled, including: employee records, personal and business bank statements, unused checks, mortgage statements, pay stubs with Social Security Numbers, copies of drivers’ licenses, and personal medical information. We found that the PII was often not identified in a timely manner and that practices for handling and disposing of the information were inconsistent in certain key respects. For example, PII that had been authorized to be destroyed, in some instances, was erroneously sent to an off-site storage facility.

We recommended that the FDIC review its existing policies, procedures, guidance, and training related to the handling and disposal of PII at ORE properties. The FDIC concurred and implemented the recommendations.

***The FDIC's Identity, Credential, and Access Management Program*** (September 2015 and follow-up report in June 2017).<sup>12</sup> Our audit from September 2015 found that the FDIC had been confronted with technical hurdles and challenges in implementing its identity, credential, and access management (“ICAM”) program. The FDIC established the ICAM program in February 2011 to address the goals and objectives of Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, which requires (among other things) that executive departments and agencies implement a government-wide standard for secure and reliable forms of credentials for eligible employees and contractor personnel to access federally-controlled facilities and information systems.

We found that despite the relatively significant investment in resources involved, the ICAM program was not subject to sufficient and consistently robust governance, which resulted in limited success. The report contained two recommendations for the FDIC to (1) define the goals and approach for implementing the ICAM program and (2) establish appropriate governance measures over the ICAM program.

---

<sup>12</sup> Copies of these reports are available at <https://www.fdicog.gov/sites/default/files/publications/15-011AUD.pdf> and <https://www.fdicog.gov/sites/default/files/publications/17-004AUD.pdf>, respectively.

In June 2017, we issued a follow-up report on the ICAM program and found that the FDIC had taken corrective actions that were sufficient for us to close the recommendations in our September 2015 ICAM Audit Report. However, there were risks warranting management's attention as the FDIC issued Personal Identity Verification ("PIV") cards to its employees and contractor personnel and enabled the cards to support access to the corporate network. Our report also noted that the FDIC had not established policies and procedures governing the management and use of PIV cards for physical and logical access and did not maintain current, accurate, and complete contractor personnel data needed to manage PIV cards. Three of the four recommendations associated with these issues have been implemented.

***The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans*** (July 2016).<sup>13</sup> This report examined an incident in which a former employee in OCFI copied, without authorization, highly confidential components of three sensitive resolution plans onto an unencrypted Universal Serial Bus ("USB") storage device, just as the employee abruptly resigned. As discussed earlier, these resolution plans contain very sensitive information. Law enforcement officials subsequently recovered the USB device containing the components of the resolution plans copied by the employee, as well as a sensitive Executive Summary for a fourth resolution plan in hard copy.

The OIG audit report identified a number of factors that contributed to the incident, including employees' access to sensitive information and employees' ability to download and store sensitive information. In addition, our report discussed indications that the employee posed a heightened security risk, including major financial problems; several disputes with FDIC management and repeated dissatisfaction; and performance management records indicating that the employee demonstrated poor judgment, lack of accountability for actions, inability to follow a supervisor's instructions, and inability to adhere to FDIC policies.

Our OIG audit report made six recommendations to better safeguard sensitive resolution plans. The FDIC implemented all of our recommendations, which included establishing an insider threat program to deter, detect, and mitigate risks posed by employees and contractor personnel; revising its policies and procedures for safeguarding sensitive resolution plans; and creating plans to test security controls periodically.

---

<sup>13</sup> This report relates to the New York Incident discussed below. A copy of this report is available at <https://www.fdicog.gov/sites/default/files/publications/16-003AUD.pdf>.

***The FDIC’s Process for Identifying and Reporting Major Information Security Incidents***

(July 2016).<sup>14</sup> This report examined the FDIC’s ability to identify and report major information security incidents under the requirements of the Federal Information Security Modernization Act of 2014 (“FISMA 2014”). As described later in this Special Inquiry report, FISMA 2014 “requires federal agencies to develop, document, and implement an agency-wide information security program that includes . . . procedures for detecting, reporting, and responding to information security incidents.”

This OIG audit focused on the FDIC’s activities, records, decisions, and reports for one particular information security incident involving a former Bank Secrecy Act (“BSA”) specialist in the FDIC’s Division of Risk Management Supervision (“RMS”). This RMS employee copied more than 1,200 documents of sensitive information, including Social Security Numbers from customer bank data, onto a single USB storage device. The files also contained sensitive Currency Transaction Reports (“CTR”) and Suspicious Activity Reports (“SAR”).<sup>15</sup> The FDIC ultimately determined that more than 100,000 files were stored on this device, which contained the information of more than 40,000 individuals who were customers at eight banks, and over 30,000 other entities.

Our OIG audit found that the FDIC’s controls did not provide reasonable assurance that “major incidents” would be identified and reported in a timely manner. The audit also determined that the large volume of potential security violations identified by the Data Loss Prevention (“DLP”) tool,<sup>16</sup> together with limited resources devoted to reviewing these potential violations, hindered meaningful analysis of the information and the FDIC’s ability to identify all security incidents, including “major incidents.”

**Suspicious Activity and Currency Transaction Reports**

Financial institutions are required to file CTRs (unless they meet certain exemption criteria) for cash transactions exceeding \$10,000. Financial institutions file SARs when transactions are suspicious in nature because they appear to involve such activity as structuring (using transactions under \$10,000 to avoid being the subject of a CTR), insider abuse, money laundering, terrorist financing, and the like. CTRs and SARs generate leads that law enforcement agencies use to initiate or help investigate money laundering, terrorist financing, and other financial crimes.

<sup>14</sup> This report relates to the Florida Incident discussed below. A copy of this report is available at <https://www.fdicog.gov/sites/default/files/publications/16-004AUD.pdf>.

<sup>15</sup> The SAR is a report filed by banks to report suspected criminal violations of federal law or a suspicious transaction related to money laundering activity, or a violation of the Bank Secrecy Act. A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to money laundering or terrorist activity.

<sup>16</sup> The DLP tool monitors and inspects FDIC data and flags potential security policy violations, including the unauthorized exfiltration of sensitive data.

During the audit, the FDIC began taking steps to prohibit employees and contractor personnel from copying data to removable media without authorization. On May 5, 2016, the FDIC CIO also outlined a series of initiatives aimed at addressing policy and program shortcomings in the FDIC's information security program, including:

- A review of all CIO Organization policies and procedures;
- The development of an Incident Response Program Guide consistent with NIST standards;
- Revision of the FDIC's Data Breach Handling Guide;
- Implementation of a new incident tracking system to automate, centralize, and enhance the management and oversight of incident response and breach-related activities;
- Restrictions on employee use of removable media;
- Restrictions on the use of printed documents that contain sensitive information;
- Implementation of Digital Rights Management software to protect the FDIC's most sensitive data; and
- Engagement of a third-party contractor to conduct an end-to-end assessment of the FDIC's IT security and privacy programs.

We have not audited or reviewed these FDIC initiatives.

The resulting OIG audit report also included five recommendations intended to strengthen the FDIC's ability to identify and report major information security incidents. The FDIC concurred with these recommendations and has implemented two of the five.

***The FDIC's Information Security Program*** (November 2016).<sup>17</sup> Our annual FISMA review in 2016 found that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, the FDIC had established policies in most of the security control areas that were reviewed, engaged an outside firm to test internal network security controls, and provided security awareness training to network users. The FDIC also restricted (with limited exceptions) the ability of network users to copy information to removable media to reduce the risk of unauthorized exfiltration of sensitive information.

---

<sup>17</sup> A summary of this report is available at <https://www.fdicoin.gov/sites/default/files/publications/17-001AUD.pdf>.

Notwithstanding these actions, we found certain security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk.<sup>18</sup> The report noted weaknesses relating to vulnerability scanning, configuration management, third-party software patching, and multi-factor authentication. It also noted that the FDIC was working to develop an overarching incident response program guide, update incident response policies and procedures, hire an incident response coordinator, better document incident investigative activities, improve the effectiveness of its DLP tool, adopt Digital Rights Management software, and hire a permanent Chief Information Security Officer ("CISO").

The report included six recommendations with which management concurred. The FDIC has implemented four of the six recommendations.

***Controls over Separating Personnel's Access to Sensitive Information*** (September 2017).<sup>19</sup>

This evaluation examined the extent to which the FDIC has established controls to mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel. The evaluation found that the FDIC could strengthen its pre-exit clearance process for employees by designating a pre-exit clearance process owner and increasing program oversight, assessing risks presented by individual separating employees, improving pre-exit clearance forms to better identify where sensitive data is located and to strengthen acknowledgments and warnings regarding breaches of sensitive information, and continuing automation efforts to develop a centralized pre-exit clearance application.

We also found that separating contractor employees may present greater risks than separating FDIC employees. For example, contractors may depart without advance notice, and the FDIC would not have sufficient time to complete its pre-exit clearance process. Further, oversight managers were not consistently signing clearance records and reviewing data questionnaires before contractors separated.

Our evaluation report included 11 recommendations intended to provide the FDIC with greater assurance that its controls mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel.

---

<sup>18</sup> FISMA states that the independent evaluations are to be performed by the agency IG or an independent external auditor as determined by the IG. The FDIC OIG engaged the professional services firm of Cotton & Company LLP to conduct this audit.

<sup>19</sup> A copy of this report is available at [https://www.fdicigoig.gov/sites/default/files/publications/17-007EV\\_0.pdf](https://www.fdicigoig.gov/sites/default/files/publications/17-007EV_0.pdf).

The FDIC concurred with our recommendations, four of which have been implemented. The FDIC advised us that three of the seven unimplemented recommendations and related corrective actions are due to be implemented throughout 2018.

***The FDIC's Processes for Responding to Breaches of Personally Identifiable Information*** (September 2017).<sup>20</sup> This audit assessed the adequacy of the FDIC's processes for (1) evaluating the risk of harm to individuals potentially affected by a breach involving PII and (2) notifying and providing services to those individuals, when appropriate.

The audit found that the FDIC established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate.

The FDIC did not complete key breach investigation activities within internally established guidelines for 13 of 18 suspected or confirmed breaches that we reviewed.<sup>21</sup> In addition, the FDIC did not notify affected individuals in a timely manner for the incidents we reviewed. Specifically, it took an average of more than 9½ months from the date the FDIC discovered the breaches to the date that the FDIC began to notify individuals. Our audit also found that (1) the rationale behind the overall impact levels assigned to the incidents were not adequately documented; (2) the underlying analysis used to support assigned impact levels for three breaches was not consistent with FDIC guidance; and (3) the overall risk ratings for five breaches were not consistent with the risk mitigation actions taken by the FDIC. Finally, we reported that the FDIC needed to strengthen controls over its Data Breach Management Team.

The FDIC had taken, or was working to take, a number of actions to strengthen its breach response processes at the time we completed the audit. However, further control improvements were needed. Accordingly, the report included seven recommendations intended to promote more timely breach response activities and strengthen controls for evaluating the risk of harm to individuals potentially affected by a breach and notifying and providing services to those individuals, when appropriate. The FDIC concurred with all of the recommendations, one of which has been implemented. The FDIC advised us that three of the six unimplemented recommendations and related corrective actions are due to be implemented throughout 2018.

---

<sup>20</sup> A copy of this report is available at <https://www.fdicigo.gov/sites/default/files/publications/17-006AUD.pdf>.

<sup>21</sup> Of the 18 suspected or confirmed breaches reviewed during the audit, 4 were also reviewed as part of this Special Inquiry.



***The FDIC's Information Security Program*** (October 2017).<sup>22</sup> Our annual FISMA audit evaluated the effectiveness of the FDIC's information security program and practices, including a review of selected security controls related to three general support systems, one business application, and the FDIC's risk management activities related to four outsourced information service providers. The audit found that the FDIC had developed an IT Strategic Plan, created a new Office of the CISO, issued PIV card credentials to its employees and contractor personnel and began requiring use of the cards, and updated a number of its information security and privacy policy directives to align with government-wide security policy and guidance.

Notwithstanding these actions, we found that the following security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk:

- The FDIC had drafted, but not yet finalized, an information security strategic plan.
- Certain network IT devices were not subject to security vulnerability scanning.
- The FDIC was using certain software in its server operating environment that was at the end of its useful life and for which the vendor was not providing support to the FDIC.
- The FDIC had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster.
- The FDIC made meaningful progress towards completing timely assessments of its outsourced service providers following the prior year FISMA audit. However, continued management attention was warranted in this area to ensure outstanding assessments were completed timely.
- The FDIC had not established an enterprise security architecture that (i) describes the FDIC's current and desired state of security and (ii) defines a plan for transitioning between the two.
- The FDIC had not installed certain patches addressing high-risk vulnerabilities on servers, desktop computers, and laptop computers within the timeframes established by FDIC policy.

At the close of the audit, the FDIC was working to strengthen the effectiveness of its information security controls in a number of other areas. For example, as it relates to this

---

<sup>22</sup> A summary of this report is available at <https://www.fdicoinig.gov/sites/default/files/publications/18-001AUD.pdf>.

Special Inquiry, the FDIC was working to strengthen its incident response capabilities by updating its breach response plan to align with OMB guidance and improving the documentation of incident investigation activities.

The report included 18 recommendations. The FDIC concurred with all of the recommendations and they are unimplemented as of January 16, 2018. The FDIC advised us that sixteen of the 18 unimplemented recommendations and related corrective actions are due to be implemented throughout 2018.

**Ongoing OIG Reviews of IT Programs.** In addition to the completed OIG reviews described above, the FDIC OIG also has several ongoing reviews regarding FDIC IT programs:

- Controls for Preventing and Detecting Cyber Threats;
- Controls over System Interconnections with Outside Organizations;
- Governance of IT Initiatives, including Enterprise Architecture and Strategic Planning; and
- Security Configuration Changes and Software Updates to the FDIC's Windows Servers

**Government Accountability Office Audits.** In its report entitled *Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent* (December 2013), the GAO recommended that the FDIC:

- Require documentation of the reasoning behind risk determinations for breaches involving PII;
- Document the number of affected individuals associated with each incident involving PII; and
- Require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices.<sup>23</sup>

The GAO has also performed relevant work regarding the integrity and reliability of the FDIC's IT programs as part of its annual audit of the FDIC's financial statements. For example, in its report entitled *FDIC Needs to Improve Controls over Financial Systems and Information* (May 2017), the GAO found that the FDIC had established a comprehensive

---

<sup>23</sup> A copy of this report is available at <http://www.gao.gov/assets/660/659572.pdf>.

framework for its information security program and implemented many aspects of its program.<sup>24</sup>

However, GAO identified certain weaknesses and stated that an underlying reason for many of these weaknesses—namely the FDIC’s implementation of access, configuration management, and information security program controls—was that the FDIC did not fully implement other aspects of its program. For example, the FDIC did not (1) include necessary information in procedures for granting access to a key financial application and (2) fully address the FDIC OIG’s finding that the FDIC did not always identify and report major security incidents in a timely manner.

This GAO report further stated that until the FDIC addressed control deficiencies and weaknesses in access controls and configuration management, its sensitive financial information and resources would remain at an increased risk of inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction—consequences that are common to the issues addressed in this Special Inquiry. The GAO concluded that the combination of the continuing and new information security control deficiencies, considered collectively, represented a Significant Deficiency<sup>25</sup> in internal controls over the FDIC’s financial reporting as of December 31, 2016.<sup>26</sup>

These reports illustrate the ongoing challenges that the FDIC faces with respect to implementing and sustaining an effective information security program. Our Special Inquiry aims to provide in-depth facts and analysis and meaningful insights and recommendations related to the cyber-security issues at the FDIC.

---

<sup>24</sup> A copy of this report is available at <http://www.gao.gov/assets/690/684999.pdf>.

<sup>25</sup> A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected, on a timely basis.

<sup>26</sup> In its report entitled, *Federal Deposit Insurance Corporation Funds’ 2017 and 2016 Financial Statements* (February 2018), GAO concluded that the FDIC did not have a significant deficiency as of December 31, 2017. A copy of this report is available at <https://www.gao.gov/assets/700/690081.pdf>.

### **III. Standards Governing the FDIC's Information Technology Security and Handling of Information Security Incidents and Breaches**

In this section, we examine the key leadership positions governing IT at the FDIC, the statutes and guidance governing incident and breach response and reporting, the FDIC's information security and privacy programs, and relevant FDIC policies and procedures in effect at the time the incidents and breaches occurred.

#### **A. Key Leadership Positions Governing FDIC Information Technology**

**Agency Head.** Under FISMA, agency heads are responsible for providing risk-based information security protections for their agency's information and information systems (including those provided or managed by another agency, contractor, or other source); complying with the requirements of the statute and related policies, procedures, standards, and guidelines; and ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes. At the FDIC, the Chairman is the agency head.

**Chief Information Officer.** The Paperwork Reduction Act of 1995 ("PRA") and the Clinger-Cohen Act of 1996 made Federal agency heads directly responsible for establishing goals and measuring progress in improving the use of IT to enhance the productivity and efficiency of their agency's operations. The statutes directed the heads of the major agencies to appoint CIOs.

The statutes assigned a wide range of duties and responsibilities to CIOs, including:

- Working with the agency head and senior program managers to implement effective information management to achieve the agency's strategic goals;
- Helping to establish a sound investment review process to select, control, and evaluate spending for IT;
- Promoting improvements to the work processes used by the agency to carry out its programs;
- Increasing the value of the agency's information resources by implementing an integrated agency-wide technology architecture; and
- Strengthening the agency's knowledge, skills, and capabilities to effectively manage information resources, deal with emerging technology issues, and develop needed systems.

The E-Government Act of 2002 also stated that CIOs are responsible for monitoring the implementation, within their respective agencies, of IT standards. In addition, FISMA directs agency heads to delegate authority to the CIO to ensure compliance with the requirements of that statute.

Martin Henning served as Acting FDIC CIO from June 2015 – October 2015. During the remaining time period relevant to this Special Inquiry, the FDIC CIO was Lawrence Gross, who assumed the position on November 2, 2015.<sup>27</sup>

**Chief Privacy Officer.** On December 8, 2004, the Consolidated Appropriations Act was enacted, and Section 522 of this Act required that each agency designate a Chief Privacy Officer (“CPO”) to assume primary responsibility for privacy and data protection policy. Key roles and responsibilities of the CPO are as follows:

- Assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form.
- Assure that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices.
- Assure that personal information contained in Privacy Act systems of record is handled in full compliance with fair information practices as defined in the Privacy Act of 1974.
- Ensure that the department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Train and educate employees on privacy and data protection policies to promote awareness of, and compliance with, established privacy and data protection policies.
- Ensure compliance with the department’s established privacy and data protection policies.

On February 9, 2016, the President issued Executive Order 13719, entitled *Establishment of the Federal Privacy Council*. This Order required that OMB issue a revised policy on the role and designation of the Senior Agency Official for Privacy (“SAOP”). The Order further stated that OMB should provide guidance as to the SAOP’s required level of expertise, adequate level of resources, and other matters.

---

<sup>27</sup> Subsequent to the work we performed for this Special Inquiry, the FDIC Board of Directors appointed Howard Whyte as the FDIC’s CIO on October 19, 2017. Mr. Gross retired from the FDIC in January 2018.

On July 28, 2016, OMB issued a revised version of Circular A-130, *Managing Information as a Strategic Resource*, to reflect changes in law and advances in technology. The revisions also ensure consistency with executive orders, presidential directives, OMB policy, and NIST standards and guidelines. As it relates to the SAOP, the Circular stated that agencies were required to designate an SAOP who had agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks. The SAOP was to have a central policy-making role and should ensure that the agency considered the privacy impact of all agency actions and policies that involve PII and ensure that the agency complied with applicable privacy requirements in statute, regulation, and policy. The SAOP was responsible for developing and maintaining a written privacy continuous monitoring (“PCM”) strategy. This privacy strategy should contain a list of the privacy controls implemented at the agency and ensure that such controls were effectively monitored on an ongoing basis. In addition, the SAOP was responsible for establishing and maintaining a PCM program to implement the strategy.

On September 15, 2016, OMB issued Memorandum M-16-24, entitled *Role and Designation of Senior Agency Officials for Privacy*. OMB Memorandum M-16-24 addressed the roles and responsibilities of the SAOP, as required by Executive Order 13719. This OMB Memorandum stated that “[e]ach agency shall develop, implement, document, maintain, and oversee an agency-wide privacy program . . . led by an SAOP who is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency’s mission.”

During the relevant time period of this Special Inquiry, the FDIC CPO and SAOP was Martin Henning, Acting (June 2015 – October 2015); and Lawrence Gross (November 2015 – October 2017).

**Chief Information Security Officer.** FISMA directed the CIO to designate a senior agency information security officer (or CISO). The CISO was responsible for:

- Carrying out the CIO’s responsibilities for information security;
- Having information security duties as the official’s primary duty;
- Heading an office with the mission and resources to assist in ensuring agency compliance with FISMA;
- Developing and maintaining an agency-wide information security program;
- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;

- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
- Assisting senior agency officials concerning their information security responsibilities; and
- Ensuring that the agency has trained personnel sufficient to assist the agency in complying with FISMA requirements and related policies, procedures, standards, and guidelines.

## **B. Statutes and Guidance Governing Incident and Breach Response and Reporting**

FISMA required each federal agency to develop, document, and implement a program to detect, report, and respond to information security incidents. Based on the statutory definition of a federal agency, the FDIC has taken the position that the FISMA statutory requirements are applicable to the FDIC.<sup>28</sup>

Pursuant to the FISMA statute, an incident is “an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.”

In 2014, the FISMA statute was amended and updated. Among other requirements, FISMA 2014 placed additional requirements upon a Federal agency to develop “procedures for detecting, reporting, and responding to security incidents,” including “notifying and consulting with, as appropriate, law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel.”

***Annual FISMA 2014 Reporting Requirements.*** FISMA 2014 required that the agency’s annual report required under the statute include a description of each “major incident” or related sets of incidents as follows:

- “[A] description of each major information security incident, or related set of incidents, including summaries of (i) the threats and threat actors, vulnerabilities, and impacts relating to the incident; (ii) the risk assessments conducted . . . of the affected information systems before the date on which the incident

---

<sup>28</sup> In a legislative analysis dated August 18, 2003, the FDIC’s Legal Division stated that “sections of the Act dealing with agency responsibilities in management and promotion of electronic government services define an agency Chief Information Officer (CIO) to include a CIO from any executive department, government corporation, government controlled corporation, or any independent regulatory agency. This definition includes the FDIC and applies to the FDIC’s CIO (44 U.S.C. § 3502). Other sections of the Act define agency as an executive agency as defined by 5 U.S.C. §§ 105 or 551; these definitions also apply to the FDIC.”

occurred; (iii) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and (iv) the detection, response, and remediation actions;”

- “[T]he total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;” and
- “[A] description of each major information security incident that involved a breach of personally identifiable information . . . including (i) the number of individuals whose information was affected by the major information security incident; and (ii) a description of the information that was breached or exposed.”

***Seven-Day FISMA 2014 Reporting Requirements for “Major Incidents.”*** FISMA 2014 also required that in the event of a “major incident,” a Federal agency must notify and consult with, as appropriate, certain Committees of Congress “not later than 7 days after the date on which there was a reasonable basis to conclude that the major incident occurred.” The statute did not specify the extent and type of information that should be contained in such a notification.

In addition, agencies must, within a reasonable period of time after additional information about a “major incident” is discovered, provide further information to the Congressional Committees. According to the statute, agencies must submit these reports to the “Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General.”

***OMB Guidance on FISMA 2014 Reporting Requirements.*** FISMA 2014 did not define the term “major incident,” but requires OMB to define the term. Under FISMA 2014, OMB was responsible for providing agencies guidance on complying with the law.

Prior to October 30, 2015, federal agencies did not have formal guidance from OMB on the definition of “major incident.” On October 30, 2015, OMB issued a Memorandum providing guidance on the fiscal year’s FISMA reporting and deadlines. This Guidance, entitled *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements* (“OMB Memorandum M-16-03”), provided a framework for agencies to use to assess whether an information security event was a “major incident.” During the relevant timeframe of this Special Inquiry, OMB Memorandum M-16-03



provided that in determining whether a “major incident” had occurred, a federal agency “shall consider” whether the incident involves:

- “[Data that] is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources;”
- “[A] high or medium functional impact to the mission of an agency;” or
- “[T]he exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either:
  - A specific threshold of number of records or users affected [10,000 or more records or 10,000 or more users affected]; or
  - [A]ny record of special importance [that is likely to result in a significant or demonstrable impact onto agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence].”

OMB Memorandum M-16-03 further indicated that “although agencies may consult with the [Department of Homeland Security’s] United States Computer Emergency Readiness Team (US-CERT) on whether an incident is considered a ‘major incident,’ it was ultimately the responsibility of the victim agency to make this determination.”

***Requirement to Update and Provide Additional Information.*** After an initial notification pursuant to the seven-day reporting requirement, OMB Memorandum M-16-03 required that the agency provide “additional information on the threats, actors, risks, previous risk assessments of the affected system, the current status of the affected system, and the detection, response, and remediation actions that were taken as soon as this information is available.”

FISMA 2014 also provided that the agency must provide notice to individuals impacted by a data breach pursuant to data breach notification policies and guidelines, which should be provided as “expeditiously as practicable and without unreasonable delay” after the agency discovers the unauthorized acquisition or access.

***FDIC Legal Division Opinion.*** On November 18, 2015, Counsel in the FDIC Legal Division’s Opinions Unit issued a memorandum on the *Applicability of OMB Memorandum M-16-03*, indicating that OMB Memorandum M-16-03 was “generally applicable to the FDIC.” In particular, the FDIC Legal Division memorandum noted:

OMB’s risk based and fact dependent approach for analyzing major incidents appears to be legally sound, providing agencies an appropriate degree of

discretion as to what constitutes a major incident. Moreover, OMB's guidance in M-16-03 regarding notice to Congress after a major incident, follow-up reporting of information to Congress as the facts become developed, and notice to impacted individuals are all in accord with the requirements of FISMA 2014.

The Legal Division memorandum concluded that "to the extent this memorandum establishes policies and practices that are valid exercises of OMB's authority under FISMA, FISMA 2014, and [National Security Presidential Directive-54/Homeland Security Presidential Directive-23], the guidance in M-16-03 imposes legally binding obligations on the FDIC."

***OMB Guidance Revising the Definition of a "Major Incident."*** On November 4, 2016, OMB issued follow-up guidance entitled *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements* ("OMB Memorandum M-17-05"). OMB Memorandum M-17-05 revised the definition of the term "major incident." The Memorandum states that a "major incident" was any incident that was likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people, and that agencies should determine the level of impact of the incident. It further stated that an unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constituted a "major incident."

OMB Memorandum M-17-05 further indicated that appropriate analysis of the incident would include the agency CIO, the CISO, mission or system owners, and if the occurrence was a breach, the SAOP. OMB Memorandum M-17-05 encouraged agencies to use the incident management process established in NIST Special Publication ("SP") 800-61, *Computer Security Incident Handling Guide* (discussed below), and encouraged use of the US-CERT National Cybersecurity Incident Scoring System, which used the following factors: Functional Impact, Observed Activity, Location of Observed Activity, Actor Characterization, Information Impact, Recoverability, Cross-Sector Dependency, and Potential Impact.

***OMB Guidance on Preparing for and Responding to Breaches.*** On January 3, 2017, OMB issued *Preparing for and Responding to a Breach of Personally Identifiable Information* ("OMB Memorandum M-17-12").<sup>29</sup> This Memorandum set forth the policy for federal agencies to prepare for and respond to a breach of PII.

---

<sup>29</sup> This Memorandum rescinds and replaces OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

It included a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. While promoting consistency, OMB Memorandum M-17-12 provided agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

***Guidance Issued by the National Institute of Standards and Technology.*** NIST SP 800-61, *Computer Security Incident Handling Guide, Revision 2*, dated August 2012, provides guidance for establishing computer security incident response capabilities and handling incidents efficiently and effectively. Among other things, NIST SP 800-61 recommended that organizations:

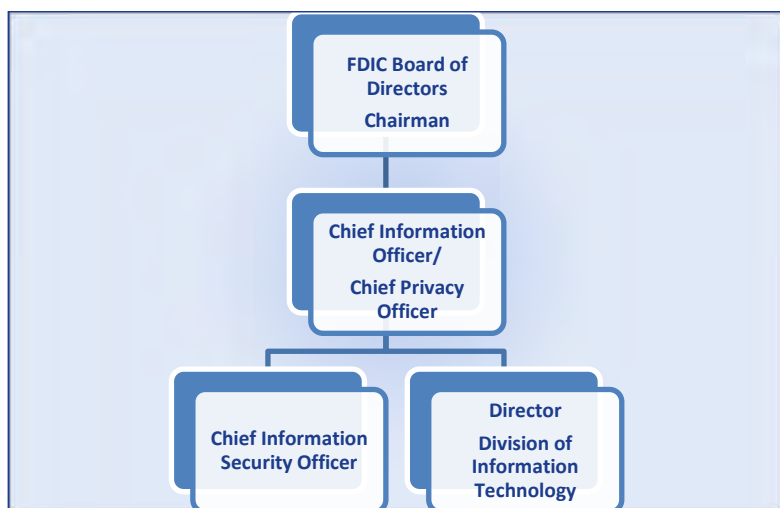
- Establish an incident response policy and a plan that provides a roadmap for implementing the incident response capability;
- Designate a single employee, with one or more alternates, to be in charge of incident response;
- Select an appropriate team structure and staffing model for handling incidents;
- Select personnel with the appropriate skills for addressing incident response;
- Provide training to incident response team members; and
- Establish metrics to measure performance and effectiveness.

With respect to notifications to potentially affected individuals, NIST SP 800-61 referred to both OMB guidance and breach notification laws enacted by states.

### **C. The FDIC's Information Security and Privacy Programs**

The FDIC's Board of Directors is responsible for the security of the FDIC's information and information systems. The FDIC's CIO, who reports directly to the FDIC Chairman, has broad strategic responsibility for IT governance, investments, program management, and information security. The FDIC's CISO, who reports directly to the CIO, is responsible for carrying out the CIO's responsibilities under FISMA—most notably, to plan, develop, and implement an agency-wide information security program. The CIO and CISO coordinate with the Director of the DIT, who reports to the CIO. The Director of DIT is responsible for managing the FDIC's IT functions.

**Figure 1: FDIC IT Governance Structure**



The FDIC’s divisions and offices also play an important role in securing information and information systems. Most divisions and offices within the FDIC have their own Information Security Manager (“ISM”), who is responsible for providing a security focus within their respective division or office and works to educate employees and contractors who have access to corporate systems and data. According to the FDIC’s *Information Security Managers Guide*, dated May 2015, the ISMs are also responsible for providing guidance to management officials regarding the Corporation’s security mission, awareness, priorities, and implementation approaches. They assess application security levels and ensure that they are maintained, prepare privacy and security risk assessment reports, and plan security requirements in new and enhanced systems. In addition, ISMs have a variety of duties relating to access control, monitoring, reporting, and enforcement.

With respect to the FDIC’s Privacy Program, the CIO was designated by the Chairman to serve as the CPO and the SAOP responsible for establishing and implementing a wide range of privacy and data protection policies and procedures pursuant to various legislative and regulatory requirements. The CPO also oversees a Privacy Program Manager, who advises on the daily operation and management of the FDIC Privacy Program.

The FDIC’s Legal Division provides advice and assistance on legal matters arising out of the administration of the FDIC information security and privacy programs, including investigation of a reported incident involving the actual or suspected loss or unauthorized disclosure of sensitive data.

## **D. The FDIC's Policies and Procedures in 2015 and 2016**

### **1. Protecting Sensitive Information**

On April 30, 2007, the FDIC instituted a directive on Protecting Sensitive Information (“FDIC Circular 1360.9”).<sup>30</sup> This Circular stated that an FDIC employee must notify the FDIC Help Desk/Computer Security Incident Response Team (“CSIRT”), the appropriate FDIC supervisor or Contract Oversight Manager, and the division or office ISM at the earliest available opportunity if it was suspected or known that PII was lost or otherwise compromised. The FDIC’s incident response was governed by the Data Breach Handling Guide (“DBHG” or “Breach Guide”) for any loss, misuse, or unauthorized access of PII.

### **2. The Data Breach Handling Guide**

At the time of the incidents discussed in this Special Inquiry report, the FDIC’s procedures for handling data breaches were set forth in the DBHG issued on April 16, 2015. The Breach Guide was designed “to ensure that the FDIC responds in a timely and appropriate manner to known or suspected data breaches, not only to protect FDIC information and assets, but also to limit harm to individuals and entities that might be affected by the incident.”

The Breach Guide defined a “data breach” as an incident where PII or sensitive business information “has been lost, compromised, acquired, disclosed, or accessed without authorization, or any similar incident where persons other than authorized users and for other than authorized purposes have access or potential access to sensitive information.” The Breach Guide further delineated a data breach as “significant” when it potentially impacted 100 or more individuals or entities.

The Breach Guide did not include procedures to identify or report “major incidents” to Congress within the seven-day requirements under FISMA 2014. A substantially similar version was re-issued on November 9, 2015. Neither provided procedures for handling “major incidents.”

The Breach Guide, and in particular, its Breach Response Lifecycle flowchart (Figure 2), was intended to serve as a roadmap for how the FDIC addresses data breaches, and includes the organizational framework, key definitions, roles and responsibilities, appropriate training, and step-by-step procedures for handling the different stages of responding to a data breach.

---

<sup>30</sup> The FDIC made changes to the directive on May 28, 2013; May 14, 2014; July 27, 2015; and October 27, 2015.

The Breach Guide further explained that the lifecycle of breach response included the following steps that flow into each other:

**Figure 2: FDIC Breach Response Lifecycle**



The following subsections summarize key roles and steps associated with the data breach response lifecycle as described in the April 16, 2015, version of the Breach Guide.

**Computer Security Incident Response Team.** When a known or suspected data breach occurred, CSIRT was to work with the FDIC employee or contractor and affected Division/Office to gather and record as much relevant information as possible. CSIRT was also responsible for notifying US-CERT about incidents involving PII within required timeframes.

**Incident Lead.** An “Incident Lead” from the Information Security and Privacy Staff (“ISPS”) within the CIO Organization (“CIOO”) would be assigned to the incident to ensure it was appropriately managed to closure. The ISPS Incident Lead reported to the CISO, who reported to the CIO/CPO. The ISPS Incident Lead and the ISM, or the Incident Response Point of Contact for the division or office affected by the incident, worked to manage the incident response. Together, they were jointly responsible for collecting information,

investigating the suspected breach, conducting a risk analysis and impact assessment, preparing a recommended course of action, and completing a document known as the Incident Risk Analysis form (“IRA”), which documented the FDIC’s actions in response to a data breach throughout its lifecycle.

**Data Breach Management Team.** A key component of the FDIC’s incident response was the FDIC’s multidisciplinary Data Breach Management Team (“DBMT”), which could be invoked to manage the FDIC’s response when an incident involving PII or agency or business sensitive information occurred. The DBMT’s membership varied based on the circumstances of the potential breach but could include the CIO/CPO; CISO; Privacy Program Manager; ISPS Incident Lead; representatives from the FDIC’s Legal Division and Office of Communications; the Chief Risk Officer; affected Division or Office Directors; ISMs; and relevant program area specialists, possibly an FDIC OIG representative,<sup>31</sup> a representative from the Office of Legislative Affairs (“OLA”), or the Internal and External Ombudsman.

The ISPS Incident Lead in the CIOO was responsible for convening the entire DBMT or a smaller subset of the DBMT depending on the circumstances of the incident. The Breach Guide indicated that the full DBMT should be invoked in the event of a suspected significant breach (over 100 individuals impacted). The role of the DBMT was to:

- Review and verify the incident risk assessment, in terms of the level of harm posed to affected individuals/entities, the financial sector (if applicable), and the Corporation;
- Determine and manage the appropriate course of action to respond to the breach and to mitigate any harm; and
- Recommend appropriate external breach communications and notification, including notification to affected individuals, banks, or other entities to the CIO/CPO or designee for approval.

The DBMT was designed to examine the facts and circumstances surrounding a particular incident, and based upon its findings, submit a recommendation to the CIO/CPO regarding an appropriate course of action, based on the risk analysis performed. The Breach Guide requires that the discussions and work of the DBMT be documented in an IRA.

---

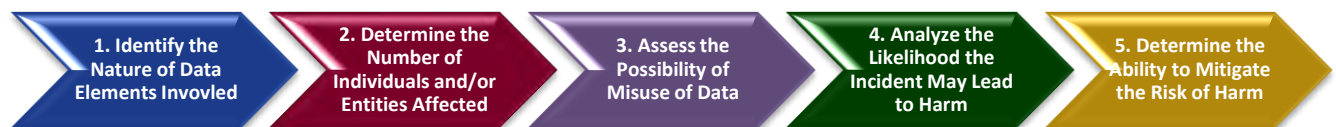
<sup>31</sup> Because the Office of Inspector General is independent from the agency and its management, the OIG is not involved in management decisions made by the DBMT. Accordingly, the FDIC OIG representative attended the DBMT meetings as a non-voting observer, in order to learn the facts being developed and assess whether the OIG should undertake further action.

**Role of Chief Information Officer and Chief Privacy Officer.** The Breach Guide indicated that the CIO/CPO was responsible for reviewing and determining whether to accept the DBMT’s recommended course of action, including breach notifications to individual consumers whose PII was compromised and provision of credit monitoring. The CIO/CPO also was to notify the Executive Office (the FDIC Chairman) and the Chief Risk Officer of the recommended course of action, including data breach notification to consumers and communications.

Notably, for “significant breaches” or breaches warranting the attention of the FDIC Executive Office, the Breach Guide required that the CIO/CPO review and determine whether or not to accept the DBMT’s recommendations within 8 hours of receipt. The CIO/CPO was to notify the Executive Office about his recommended course of action prior to the release of external breach notification. Notification would be made to affected parties, which could include individuals, entities, and third parties.

**Incident Risk Analysis and Impact Assessment.** In order to assess the potential impact of a breach and determine the appropriate course of action, the ISPS Incident Lead, in coordination with the ISM, would perform an incident risk analysis/impact assessment, using the following five-factor risk assessment methodology as a guide.

**Figure 3: Five Factors of Risk Assessment Methodology**



Source: DBHG, Version 1.4, dated April 16, 2015.

The Breach Guide noted that this methodology was based on OMB guidance and NIST risk assessment guidelines, which utilize the impact levels of Low, Moderate, and High to rate the potential harm that could result if data were inappropriately accessed, used, or disclosed.

Using the above methodology, the ISPS Incident Lead and ISM would assess each of the five factors identified above in relation to the specific incident. They would then balance the five factors collectively and assign an overall risk determination level (Low, Moderate, or High) to the incident. In assessing the five factors, according to the DBHG, the following questions were to be considered:

- What is the likely risk of harm?
- Was the loss intentional?



- Was the compromised data deliberately targeted?
- What was the sensitivity level of the data involved in the incident? For example:
  - Was sensitive bank exam, charter, or closing information compromised?
  - Was sensitive personal information, financial information (e.g., credit card numbers), or Social Security Numbers lost/stolen or otherwise compromised?
- In what medium (paper, email, thumb drive, system, etc.) was the data maintained, and what associated controls (encryption, password-protection, etc.) were in place?
- Could the lost/stolen/compromised information be used to perform identity theft or cause other harm to entities or individuals?
- Could the lost/stolen/compromised information damage the reputation or cause a financial loss to entities or individuals?
- How many individuals or parties were affected?
- Are the identities of the affected individuals or parties known?

***Incident Risk Analysis Form.*** The ISM was responsible for documenting the findings of the investigation and the impact assessment in an IRA. The purpose of the IRA was to assess and assign an overall potential impact/severity level (Low, Moderate, or High) to an actual or potential data breach. In addition, the IRA was used to determine and document corrective actions and recommended mitigation measures, including whether external notification was recommended, to mitigate the harm posed by the incident. The ISPS Incident Lead was responsible for reviewing the IRA, working with the ISM to make any adjustments to the form, and making a final determination about the appropriate risk level (Low, Moderate, or High) and breach/non-breach designation for each incident.

***Invoking the DBMT.*** The DBHG stated that all incidents require attention, but their risk, characteristics, expected outcomes, and the level of effort and resources needed to respond may vary. In performing this analysis, the ISPS Incident Lead would decide whether to invoke the entire DBMT or a smaller, specialized version of the DBMT to determine the recommended course of action and manage the incident to closure.

***Incident Mitigation.*** Based upon the risk analysis performed in the previous steps, the DBMT would determine and recommend to the CIO/CPO (or designee) an appropriate course of action that included strategies to mitigate the impact of the incident. The FDIC would aim to mitigate any harmful effect that was known to have occurred as a result of a use or disclosure of sensitive information, including sensitive bank information or PII, in

violation of federal requirements and the FDIC's data security/privacy protection policies and procedures.

According to the DBHG, the following factors were to be considered when determining the need to mitigate any damages:

- Whether any damage occurred;
- The nature of the damage that occurred;
- The amount of damage;
- The type of data that was used or disclosed;
- The reasons for the disclosure; and
- Whether the harm can be mitigated.

The DBHG provided the following examples of possible techniques for mitigation:

- Notification to affected individuals and entities;
- Provision of credit monitoring services to affected individuals and entities; and
- Use of the FDIC Call Center to assist affected individuals and businesses.

***Process for External Notifications to Affected Individuals.*** The DBHG stated that authorization by the Executive Office and CIO/CPO was required prior to issuing or conducting external communications or notifications regarding potential or known data breaches. Before issuing an external notification, the FDIC had to first determine the scope of the breach and, if applicable, restore the reasonable integrity of the compromised system or data. The goal was to provide notification to affected individuals/entities without unreasonable delay (generally within 10 days from the date that the analysis of the breach was completed), so that affected individuals and entities could take protective steps quickly.

In addition, the timing of the notification had to be appropriate and consistent with the needs of law enforcement, national security (if applicable), and any measures necessary for the FDIC to determine the scope of and contain the breach. The CIO/CPO (or designee) and/or the Executive Risk Committee could decide to delay notification after weighing the impact on affected individuals and parties, internal operations, and other relevant stakeholders or entities.

According to the DBHG, notifications to affected parties depended upon the circumstances and did not always include remediation assistance such as an offer of credit monitoring services. In general, the FDIC was to provide external notification and credit monitoring for

moderate or high incidents where Social Security Numbers or other sensitive information that could lead to identity theft had been compromised.

**DBHG Updates.** The Breach Guide was re-issued on December 23, 2015, to reference OMB Memorandum M-16-03, provide OMB’s framework for assessing “major incidents,” recognize the requirement of notifications to Congress, and set forth procedures for handling “major incidents.” In early February 2016, then-CIO Lawrence Gross (“then-CIO Gross”) ordered that it be removed from the FDIC intranet and that the prior Breach Guide from April 16, 2015, be re-posted, because then-CIO Gross had not reviewed or approved the new version, nor had it received adequate input from other stakeholders, such as the Legal Division and the Division of Administration’s Human Resources Branch. On June 6, 2016, then-CIO Gross published an interim update to the DBHG that referenced FISMA 2014 and OMB Memorandum M-16-03 for considering external incident notification steps.

On April 7, 2017, the DBHG was reissued as the “Breach Response Plan.” This Plan clarified the definition of when an actual or suspected breach is considered major under OMB Memorandum M-17-05. It also added reference to “major incident” requirements, where applicable. In July 2017, the FDIC created an Incident Response Plan, a separate document from the Breach Response Plan, which serves as a top-level document governing each stage of the FDIC’s incident handling lifecycle. In October 2017, the FDIC again updated the Breach Response Plan to align with OMB Memorandum M-17-12.

### **3. The FDIC’s Data Loss Prevention Tool**

The incidents discussed in this Special Inquiry Report were detected by the FDIC through its DLP tool. Prior to September 2015, the DLP tool was configured to detect data exfiltration that occurred through open file shares on the internal network and network events (i.e., e-mail and web updates) only.

As discussed previously, the FDIC OIG recommended in our report, *The FDIC’s Process for Identifying and Reporting Major Information Security Incidents* (July 2016), that the FDIC review the implementation of the DLP tool to determine how the tool could be better leveraged to safeguard sensitive information and identify and mitigate “major incidents.” The FDIC has taken steps to implement this recommendation, and it is now closed.

### **4. The FDIC’s Pre-Exit Clearance Procedures for Separating Employees**

On September 3, 2014, the FDIC issued Circular 2150.1, which established procedures for employees separating from employment with the FDIC. As part of these procedures, separating employees were required to complete and sign a standard form entitled *Pre-Exit*

*Clearance Record for Employees* (“Pre-Exit Clearance Form”). A copy of this form is available in Appendix III. By signing this record, the employee certified that:

I have not removed any **Confidential Information** ... from FDIC premises except as necessary or appropriate in the course of my employment, disclosed any **Confidential Information** to any person not authorized to receive it, nor sent any **Confidential Information** to any address outside the FDIC (whether by mail, email or otherwise) except in accordance with applicable FDIC policies on the use and transmittal of FDIC information, and (ii) I have returned to the FDIC all **Confidential Information** that I possessed (in whatever form it existed) and will not transmit or remove (in any format or in any medium) any **Confidential Information** to any address outside the FDIC between the signing of this certification and my departure from FDIC employment.

The Pre-Exit Clearance Form stated that “Confidential Information” meant information that an employee came to possess by virtue of his/her employment with the FDIC that was or had been confidential either (i) of a personal nature (PII) or (ii) as it relates to certain commercial interests, to banking or financial institutions or the banking or financial industry in general, or to the overall programs and mission of the FDIC (sensitive information).

The form further provided that in the event of a breach of this agreement, the FDIC would be entitled to injunctive relief and other remedies available under the law as well as the recovery of reasonable costs and attorneys’ fees in connection with obtaining any such injunctive relief. Finally, by signing the form, the employee acknowledged that his or her statements on the form were:

[T]rue, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (see 18 U.S.C. [Section] 1001).

As part of the pre-exit clearance process, the separating employee’s immediate supervisor had to ensure that the employee completed FDIC Form 2150/03, *Data Questionnaire for Departing/Transferring Employees/Contractors* (“data questionnaire”). A copy of this form is available in Appendix IV. The data questionnaire had to be completed at least 1 week, but no more than 30 days, prior to the employee’s separation. This form required the separating employee to identify the location of paper and electronic records in his/her possession, access to information technology network shared folders and SharePoint sites, and any email folders that the separating employee shared with other FDIC personnel.

## 5. The FDIC's Policies and Procedures for Responding to Congressional Requests and Executing Legal Holds

This Special Inquiry examined the FDIC's responsiveness to requests from the SST Committee for documents and information related to information security incidents and breaches and the FDIC's policies and procedures for safeguarding and handling sensitive information housed on FDIC systems.

***Congressional Contacts and Correspondence.*** On November 9, 2011, the FDIC established a directive describing the "procedures for handling verbal and written contacts between FDIC staff and Members of Congress and Congressional Staff" ("FDIC Circular 1211.2"). According to FDIC Circular 1211.2, OLA was to act as a central contact point for Members and their staff who had inquiries relating to the work of the FDIC. With respect to Congressional correspondence, OLA was to determine which FDIC division or office would be responsible for preparing a draft response to be signed by the Chairman or the Director of OLA.

***Legal Hold Policy and Implementation.*** On September 5, 2012, the FDIC established a directive relating to its policy for placing a legal hold to preserve FDIC documents and records ("FDIC Circular 5500.5"). This Circular placed the responsibility for legal holds on the Legal Division, which issued Legal Hold Guidelines (revised in June 2013).

The Legal Hold Guidelines emphasized the importance of legal holds by stating:

In any matter involving requests for the FDIC's documents, whether the FDIC is the plaintiff or defendant in a lawsuit, or in the receipt of a Congressional or other subpoena, the FDIC has an obligation to produce materials in its possession, custody and control that bear on the issues in that matter.

### Legal Hold

FDIC Circular 5500.5 defines a legal hold as a suspension of the routine disposal of paper and electronic documents, data, and other records in any format that may be potentially relevant to litigation or other matters in which documents must be produced.

The Legal Hold Guidelines stated further that "[i]mplementation and compliance with legal holds ensure that the FDIC meets its obligations to the Courts, Congress, and opposing parties..."

The Legal Hold Guidelines "describe the procedures for requesting, issuing, implementing, and removing a legal hold on FDIC records and information." These Guidelines also defined the scope and process for establishing legal holds requiring the preservation of relevant documents from "key players," including FDIC employees who created relevant documents

or had personal knowledge about issues in the underlying matter. The Legal Division was responsible for identifying key players in a particular matter.

#### IV. Factual Circumstances of the Handling of Information Security Incidents and Breaches at the FDIC

This Section presents the factual circumstances of the eight information security incidents at the FDIC in late 2015 and early 2016. The eight incidents and the relevant events are listed below in Table 1.

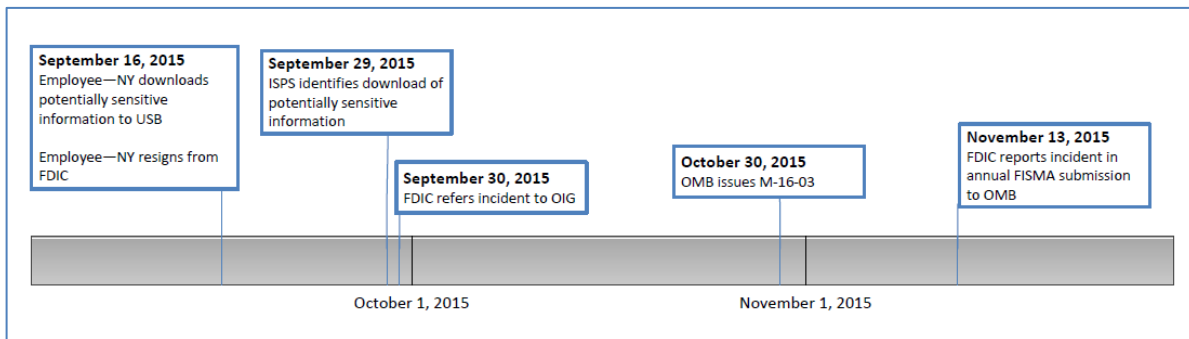
**Table 1: Key Dates Associated with the Eight Incidents**

Incident	Dates Incident Detected by the DLP Tool	Date of Employee's Departure From FDIC	Date that FDIC Discovered the Incident	Notification Decision	Date Individuals Began to be Notified	Days from Notification Decision Until Beginning of Notifications	Potentially Affected Individuals
New York	9/16/15	9/16/15	9/29/15	N/A*	N/A	N/A	0
Florida	9/16/15 9/17/15 10/15/15	10/15/15	10/23/15	5/12/16	11/12/16	184	20,528
Incident A	9/30/15 10/1/15	10/23/15	11/10/15		11/12/16	184	4,884
Incident B	10/29/15	10/30/15	11/10/15		11/15/16	187	1,907
Incident C	11/15/15	11/27/15	12/10/15		12/13/16	215	33,969
Incident D	11/1/15 12/2/15	12/31/15	1/8/16		11/11/16	183	11,931
Incident E	12/28/15	12/31/15	1/7/16		11/14/16	186	11,417
Incident F	1/31/16 2/1/16 2/24/16 2/25/16	2/26/16	2/29/16		11/15/16	187	36,997
<b>Total</b>							<b>121,633</b>

\* No individuals' PII was involved in this incident, so consumer notification was not needed. However, the Deputy Director of the Complex Financial Institutions Group within RMS told us he notified the institutions whose resolution plans were breached between 9/29/16 and 10/2/16 by telephone.

Details regarding how the incidents occurred, the data involved, and the manner and timeframes in which the FDIC responded to each incident follow.

## A. The New York Incident



**Figure 4: Timeline for New York Incident**

On September 29, 2015, the FDIC learned that Employee-NY,<sup>32</sup> a former OCFI employee who had abruptly resigned on September 16, 2015, took highly sensitive components of SIFI resolution plans, which, as noted earlier, are referred to as “living wills.”

The “living wills” generally contain sensitive information, including information about critical vendors, suppliers, and associated agreements that SIFIs maintain; a description of the actions that SIFIs would undertake to support clients and vendors under stress; non-public financial and business data; personal information about employees; the location and activities of data centers; and a list of critical operations. FDIC OIG law enforcement officials subsequently recovered the USB device containing the components of three of the resolution plans copied by Employee-NY, as well as a sensitive Executive Summary for a fourth resolution plan in hard copy.

As noted previously, our OIG report entitled *The FDIC’s Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* identified indications that Employee-NY posed a heightened security risk, including major financial problems that raised serious questions about the employee’s suitability to work for the FDIC; several disputes that the employee had with FDIC management and repeated express dissatisfaction; and performance management records that showed the employee demonstrated poor judgment, lack of accountability for actions, inability to follow a supervisor’s instructions, and inability to adhere to FDIC policies.

In addition, before departing the FDIC, Employee-NY completed the Pre-Exit Clearance Form, attesting that she had returned to the FDIC all confidential information she

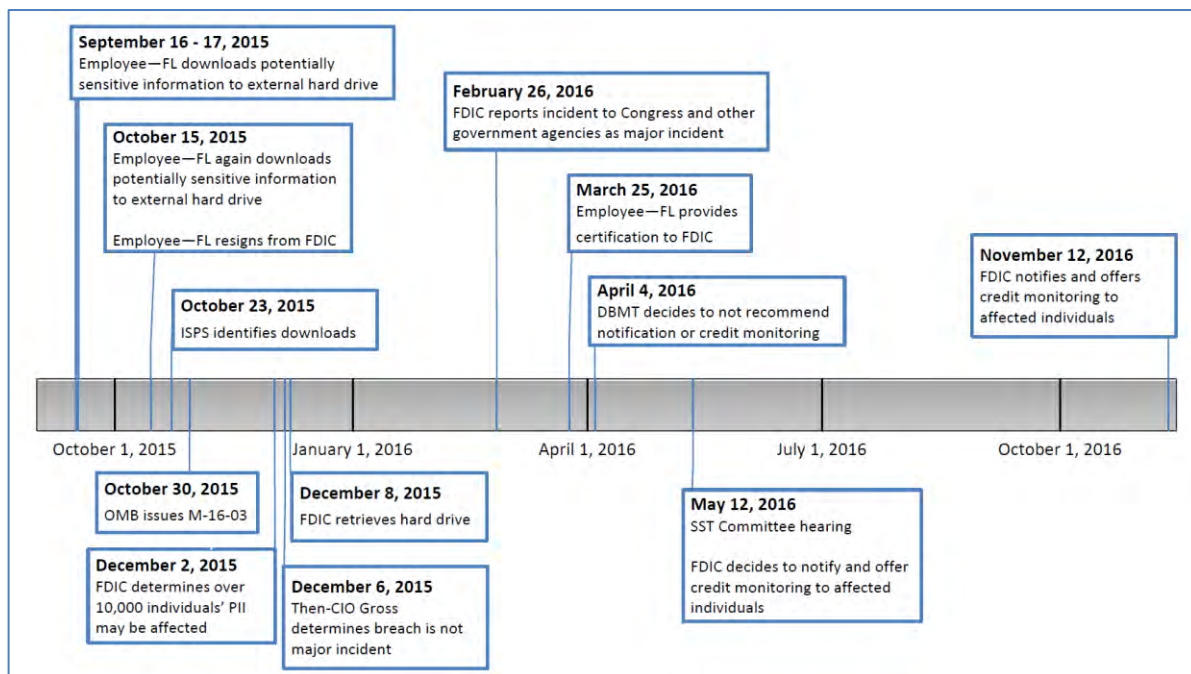
<sup>32</sup> Throughout this Special Inquiry report, we refer to the former FDIC employees by incident to protect their privacy.

possessed and would not remove any confidential information from the FDIC before her departure.

The FDIC notified the financial institutions impacted by this incident.<sup>33</sup> The FDIC also included the New York Incident in its annual FISMA submission that was transmitted to OMB in November 2015 and ultimately to Congress in March 2016.

The FDIC referred the New York Incident to the OIG, and the OIG conducted an investigation to determine whether any potentially criminal conduct had occurred. Based on the OIG’s investigation, on March 15, 2018, an indictment was filed against Employee-NY for theft of government property (Title 18, United States Code, Section 641) in the Eastern District of New York (Indictment, *United States v. Aytes*, No. 18-cr-00132 (E.D.N.Y. March 15, 2018)).

## B. The Florida Incident



**Figure 5: Timeline for Florida Incident**

Our OIG audit entitled *The FDIC’s Process for Identifying and Reporting Major Information Security Incidents* reviewed the FDIC’s activities, records, decisions, and reports for one breach, referred to as the Florida Incident. On October 23, 2015, the FDIC ISPS employee reviewing DLP tool hits of departing employees learned that on September 16-17 and

<sup>33</sup> Customer notifications were not required because the incident did not involve PII.



October 15, 2015, Employee-FL, a former FDIC employee in RMS, downloaded over 1,200 documents containing sensitive information, including confidential information regarding the FDIC's examination of financial institutions, customer Social Security Numbers, SARs, and other financial institution files, onto a removable media device.

Examination reports and examination-related material may include the following information: individuals' Social Security Numbers, full names, dates of birth, home addresses, home phone numbers, employment information, loan numbers, or outstanding loan amounts; taxpayer identification numbers/employer identification numbers; account numbers; Reports of Examination; loan trial balances; investigative reports; consent orders; Call Report data; pre-exam planning memoranda; visitation memos; examination call-in memos; FinCEN downloads; automated clearinghouse information; or audit reports.

By reviewing Employee-FL's FDIC-issued computer, an FDIC ISPS employee determined that Employee-FL used a personally-owned removable media device that the FDIC did not have in its possession to download the data. Prior to her departure from the FDIC, Employee-FL had signed the FDIC's Pre-Exit Clearance Form, certifying she had not taken confidential information.

On November 19, 2015, Employee-FL and her FDIC supervisors had three discussions, by telephone, where she denied copying the information or owning a removable media device. Over the next two weeks, Employee-FL refused to meet with FDIC staff. She eventually advised them that any further communication from the FDIC should be directed to her private legal counsel. The FDIC also learned that Employee-FL had obtained employment with a financial services company based in India and that she was experiencing personal hardship as she was in the midst of a divorce and had lost her residence.

On December 2, 2015, the FDIC determined that the Florida Incident involved more than 10,000 unique Social Security Numbers. Accordingly, the incident met the threshold in OMB Memorandum M-16-03 for 7-day reporting under FISMA 2014. Despite several emails from Information Security staff inquiring as to when another DBMT meeting would occur, in a memorandum dated December 6, 2015, then-CIO Gross stated that the Florida Incident did not constitute a "major incident" under OMB Memorandum M-16-03.<sup>34</sup> This decision was made without the benefit of a recommendation from the DBMT. Then-CIO

---

<sup>34</sup> On December 7, 2015, at the request of then-CIO Gross, ISPS added an attachment to the memorandum that contained a timeline of events related to the Florida Incident. The memorandum itself, including then-CIO Gross' "major incident" determination, did not change.

Gross further stated that “additional work is required by RMS, Legal, and ISPS before the impact level of the breach can be determined.”

Subsequently, the FDIC learned that Employee-FL’s attorney had taken possession of the personally-owned removable media device. The FDIC obtained the device from the attorney on December 8, 2015, more than 11 weeks after the first download of information. The FDIC did not determine whether and in what manner the data was accessed, copied, or disseminated.

**Protecting Sensitive Information**

FDIC Circular 1360.9 states that, in order to protect sensitive information, it is the policy of the FDIC to safeguard sensitive information from unauthorized access. The Circular requires that sensitive information not be removed from the workplace without prior management approval. The attorney’s possession of the device constituted unauthorized access as only those individuals who have a legitimate need to access sensitive information in the performance of their duties shall be provided access.

On February 19, 2016, during the course of our audit work on the Florida Incident, the OIG advised the FDIC that it should have reported the Florida Incident as a “major incident” to Congress, in accordance with FISMA 2014 and OMB Memorandum M-16-03:

[T]he incident should have been reported to the Congress not later than December 9, 2015 – 7 days after it was determined that more than 10,000 unique [Social Security Numbers] were involved in the breach . . . Moreover, it is possible that the incident could have been designated as major as early as November 6, 2015 [7 days after OMB issued its Memorandum M-16-03], as the exfiltration involved records that had special importance.<sup>35</sup>

The FDIC subsequently reported the incident to Congress and other appropriate government agencies pursuant to FISMA 2014 on February 26, 2016 (see Appendix VI). Then-CIO Gross later stated, on June 20, 2016, that “[a]fter receiving the OIG’s February 19, 2016 memorandum, we adopted their analysis and conclusions and have since then reported consistent with it.”

On March 25, 2016, Employee-FL’s attorney provided the FDIC with a signed statement from Employee-FL, which stated that since departing from the FDIC, Employee-FL had not “disseminated or copied any FDIC Confidential Information from the [USB drive] and no

---

<sup>35</sup> The information downloaded by the employee included SARs. Inappropriate disclosure of a SAR to an unauthorized person is a violation of federal law. Such disclosure could result in significant or demonstrable impact to public confidence in the FDIC’s ability to protect personal information since SARs often contain PII. The IRA for this incident noted that the downloaded information could be used to open new accounts or commit identity theft, and could be used to cause public/reputational embarrassment, jeopardize the mission of FDIC, or cause other harm.

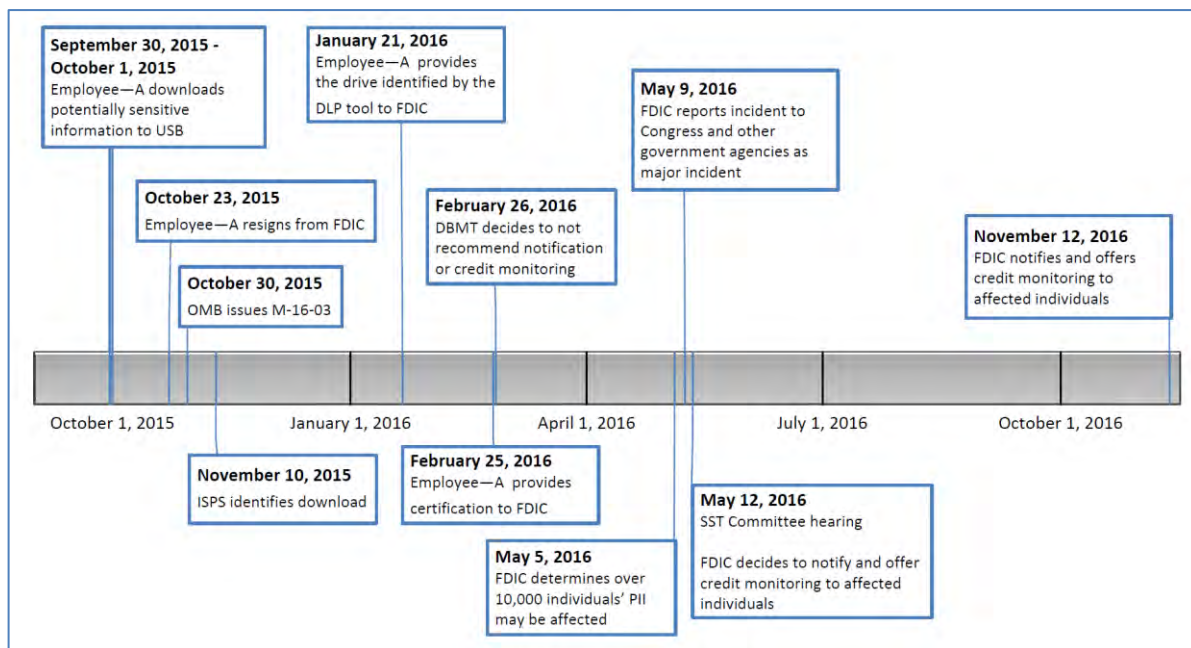
longer [had] in [her] possession, custody or control any FDIC Confidential Information in any format” (see Appendix V, page 125).

On April 4, 2016, the DBMT determined that the incident was “low risk” based on “mitigating factors.” Given this determination, the DBMT did not recommend that bank customers be notified, nor did the DBMT recommend credit monitoring for such individuals. The IRA for this incident included a partially completed risk analysis/impact assessment—the overall sensitivity of the data was classified as high; however, no risk level was assigned for overall probability of misuse, overall likelihood of harm, and overall ability of the FDIC to mitigate harm. The IRA did not indicate for this incident, nor did any of the IRAs for the other incidents examined in this Special Inquiry report, how these individual risk factor determinations led the DBMT to the overall risk designation for the incident.

Based on our interviews, we determined that on May 12, 2016, after testifying before the SST Committee’s Subcommittee on Oversight, then-CIO Gross met with FDIC Chairman Martin Gruenberg (“Chairman Gruenberg” or “the FDIC Chairman”); Chief Operating Officer Barbara Ryan (“COO Ryan”); OLA Director Andy Jiminez (“OLA Director Jiminez”); and Barbara Hagenbaugh, Deputy to the Chairman for Communications, to discuss the hearing. They discussed notifying individuals potentially affected by the breach and the related concerns brought up in the Congressional hearing that day. Based on this discussion, the group reached a consensus and the FDIC Chairman made the decision to notify individuals and provide credit monitoring. Then-CIO Gross, in turn, advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. The FDIC ultimately determined that the PII of 20,528 individuals was involved and began notifying consumers and offering credit monitoring to those individuals on November 12, 2016, more than a year after the information was downloaded.

The OIG referred this matter to the U.S. Attorney’s Office in the Middle District of Florida for prosecutorial consideration. On June 1, 2017, the U.S. Attorney’s Office declined prosecution.

## C. Incident A



**Figure 6: Timeline for Incident A**

On November 10, 2015, the FDIC learned that Employee-A, a former RMS employee, had downloaded more than 500 documents containing sensitive information to a removable media device on September 30 and October 1, 2015. The documents included FDIC examination-related material, including confidential Reports of Examination. Prior to his separation from the FDIC, Employee-A had signed the FDIC's Pre-Exit Clearance Form, certifying that he had not taken confidential information.

On November 25, 2015, Employee-A's former supervisor contacted him about the matter, and Employee-A turned in an FDIC-issued removable media device on November 30, 2015 – approximately 2 months after the information was downloaded. Employee-A stated that he had taken the data in case he returned to the FDIC to work.

On December 16, 2015, the FDIC learned that the device Employee-A returned did not match the device that the DLP tool had identified. Employee-A falsely asserted that there was “no other USB drive for the FDIC to review.” In a later conversation, Employee-A claimed, again falsely, that the FDIC data was on the FDIC-issued device he had already returned and not on a personal device.

On December 23, 2015, the DBMT decided that Employee-A's former supervisor, the then-CISO Christopher Farrow (“then-CISO Farrow” or “Mr. Farrow”), and FDIC Legal Division staff would call Employee-A again. When Employee-A's former supervisor later tried to arrange the call, Employee-A refused to speak to then-CISO Farrow and Assistant General

Counsel Henry Griffin (“AGC Griffin”). AGC Griffin explained in an email to then-CIO Gross on January 11, 2016, that Legal Division attorneys had prepared a demand letter to send to Employee-A, since he was being “uncooperative when we tried to reason with him by telephone in the last week of December.” On January 21, 2016, Employee-A turned in his personally-owned device, which contained the compromised data and matched the device detected by the DLP tool.<sup>36</sup>

On February 11, 2016, the FDIC contacted Employee-A to confirm that he had not copied or disseminated the data, among other things. On February 25, 2016, over 3 months after the FDIC discovered the breach and nearly 5 months after the information was downloaded, Employee-A signed a statement asserting that he did not “make any electronic copies of [the personally-owned drive], nor did [he] copy any Confidential Information from the [the personally-owned drive] onto another computer or electronic storage device” (see Appendix V, pages 126-127). According to the IRA for Incident A, Legal Division staff determined that the statement was sufficient in responding to the Legal Division’s concerns discussed with Employee-A on February 11.

On February 26, 2016, the DBMT determined that the incident was a breach with “low risk” of harm and, therefore, it neither recommended consumers be notified nor credit monitoring be offered. The IRA for this incident contained a completed risk analysis/impact assessment, which classified the overall data sensitivity as moderate, the overall probability of misuse as low, the overall likelihood of harm as moderate, and the overall ability of the FDIC to mitigate harm as able to mitigate most harm.

On April 29, 2016, nearly 5½ months after the FDIC first discovered the downloads, RMS completed its review of all but one file involved in the incident. On May 5, 2016, the FDIC determined that the files could include the PII or sensitive information of over 10,000 individuals, although the count was still ongoing at that time. The FDIC reported the incident to Congress and other appropriate government agencies on May 9, 2016, over 7 months after the information was downloaded (see Appendix VI).

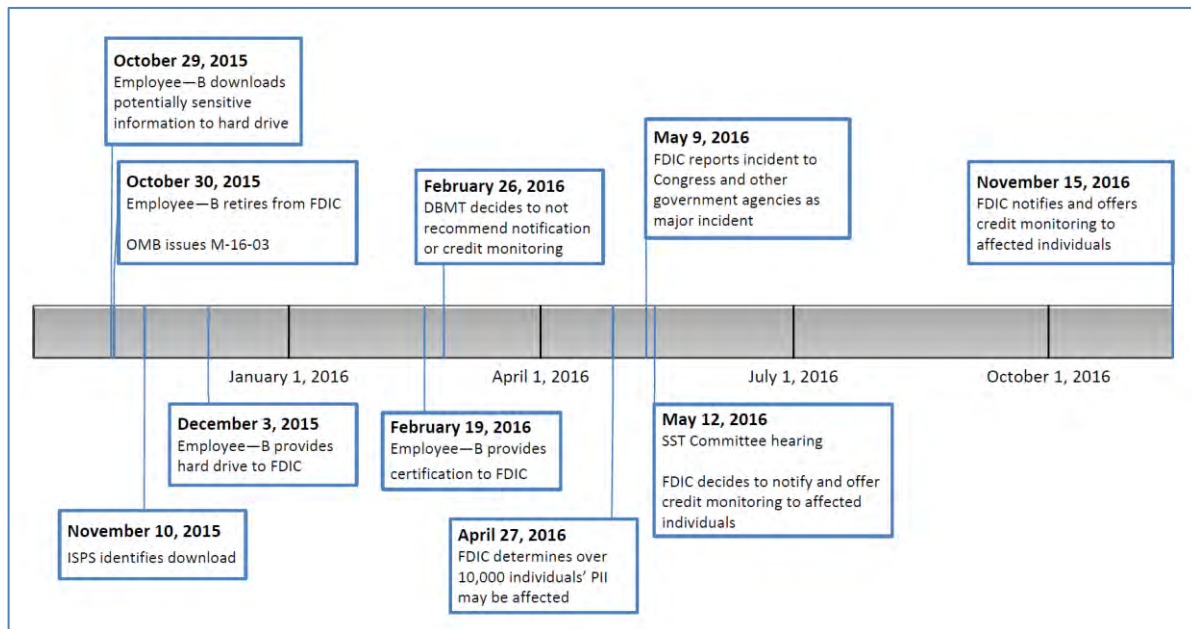
As with the Florida Incident, on May 12, 2016, after testifying before the SST Committee’s Subcommittee on Oversight and meeting with the FDIC Chairman, then-CIO Gross advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. Subsequently, after further analysis, the FDIC determined that

---

<sup>36</sup> When subsequently interviewed about the data breach by OIG investigators, Employee-A said that he had copied the data from his personal device to the FDIC-issued device, because the personal drive was his personal property and it contained personal files. He said he copied them directly from one drive to the other; he did not copy them to his computer and then onto the second drive. Employee-A did not consent to a search of his personal computer but insisted that he did not have any FDIC information there.

the PII of 4,884 individuals was involved, and began offering credit monitoring to those individuals on November 12, 2016 – over 1 year after the information was downloaded.<sup>37</sup>

## D. Incident B



**Figure 7: Timeline for Incident B**

On November 10, 2015, the FDIC learned that Employee-B, a former RMS employee, had downloaded more than 1,200 documents containing sensitive information to a USB drive on October 29, 2015. Employee-B took data including bank examination information, SARs, and confidential Reports of Examination, among other things. Prior to his separation from the FDIC, Employee-B had signed the FDIC’s Pre-Exit Clearance Form, certifying that he had not taken confidential information.

After his departure, Employee-B’s former supervisor in RMS contacted him, and on December 3, 2015, Employee-B provided a personally-owned external hard drive to his former FDIC supervisor. He stated that he “mistakenly” copied the wrong folder to the personally-owned hard drive and had only accessed it to confirm that the data in question

<sup>37</sup> In each instance where the FDIC notified the customers and offered credit monitoring services, the FDIC performed further research, including contacting financial institutions to obtain addresses for individuals initially determined to be potentially affected. In the course of doing so, the FDIC learned that the initial estimated figure was incorrect. This resulted in the final number of individuals notified being substantially lower.

had been downloaded.<sup>38</sup> On December 17, 2015, the FDIC confirmed that the hard drive provided by Employee-B was the same as the drive identified in the DLP report.

On February 19, 2016, about 3½ months after Employee-B downloaded the information, he returned a signed statement indicating that he had not stored the data anywhere other than the drive; no one else had access to the drive; the data had not been accessed, copied, downloaded, or disseminated in any way; and that he would further refrain from accessing or disclosing the information (see Appendix V, pages 128-129).

On February 26, 2016, the DBMT determined that the breach was “low risk” and therefore did not recommend notifying customers or offering credit monitoring services. The IRA included a completed risk analysis/impact assessment that classified the overall data sensitivity as moderate, the overall probability of misuse as low, the overall likelihood of harm as low, and the overall ability of the FDIC to mitigate harm as able to mitigate most harm.

On April 27, 2016, almost 6 months after the information was downloaded, the FDIC determined that the PII or sensitive information of more than 10,000 individuals or entities was potentially involved in Incident B. Two days later, the FDIC completed its review and found that the sensitive records of 28,232 individuals and entities were potentially affected. The FDIC notified Congress and other appropriate government agencies of this incident on May 9, 2016, more than 6 months after the information was downloaded (see Appendix VI).

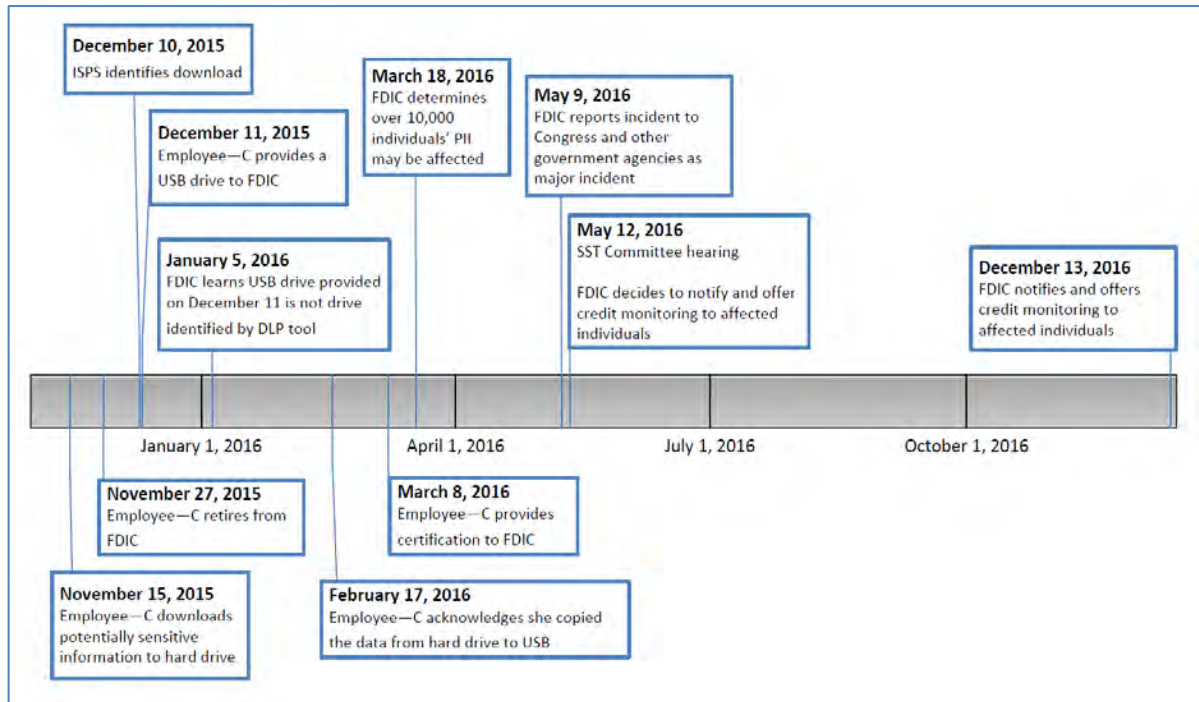
On May 12, 2016, after testifying before the SST Committee’s Subcommittee on Oversight and after meeting with the FDIC Chairman, then-CIO Gross advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. In its preparations for doing so, the FDIC determined that the final number of individuals to be notified and offered credit monitoring was 1,907.<sup>39</sup> The FDIC began to notify bank customers on November 15, 2016, more than 1 year after the information was downloaded, and offered credit monitoring to those individuals.

---

<sup>38</sup> When later interviewed about the breach by OIG and FinCEN investigators on September 21, 2016, Employee-B did not consent to a search of his personal computer.

<sup>39</sup> See footnote 37.

## E. Incident C



**Figure 8: Timeline for Incident C**

On December 10, 2015, the FDIC ISPS employee reviewing DLP information discovered that Employee-C, a retiring Division of Depositor and Consumer Protection (“DCP”) employee, had copied sensitive information to a removable media device on November 15, 2015, before her last day in the office on November 25, 2015. The data Employee-C downloaded included a bank’s loan trial balance, which could include sensitive information such as loan numbers and unpaid balances. The ISM initially estimated that approximately 388 files had been compromised and copied, including approximately 28,000 Social Security Numbers as well as borrower names, addresses, loan numbers, and outstanding loan balances. Prior to her separation from the FDIC, Employee-C had signed the FDIC’s Pre-Exit Clearance Form, certifying that she had not taken confidential information.

On December 10, 2015, Employee-C’s former FDIC supervisor in DCP contacted her about the breach. As reflected in the IRA, the supervisor reported that Employee-C had “inadvertently” copied some of the files that were flagged by the DLP tool while trying to copy personal files.<sup>40</sup> Employee-C returned a personally-owned flash drive to the FDIC the following day.

<sup>40</sup> Employee-C was later interviewed by OIG and FinCEN investigators on September 20, 2016. In that interview, Employee-C again indicated that she accidentally copied the files.



On January 5, 2016, Employee-C's former supervisor reported that neither this drive nor the FDIC-issued flash drive Employee-C turned in during her separation process were the removable media device that the DLP tool had detected. The personally-owned flash drive, however, contained the files that the DLP tool detected as those Employee-C had downloaded before she left the FDIC.

On February 3, 2016, the DBMT recommended that ISPS conduct further forensic review to reexamine whether either of the flash drives matched the drive identified by the DLP tool. ISPS determined that Employee-C used an external hard drive, not a flash drive, to download the data.

When Employee-C's former FDIC supervisor in DCP confronted her with the findings of the additional forensic review, Employee-C admitted that she had used an external hard drive to download data and that she had not returned it to the FDIC. Employee-C stated that once her former FDIC supervisor had contacted her to ask about the data, she copied the downloaded data from the external hard drive to the personally-owned flash drive that she returned to the FDIC on December 11, 2015.<sup>41</sup>

This explanation raised concerns that Employee-C used a non-FDIC computer to copy the data from the hard drive to a flash drive, which could result in some of the sensitive FDIC data remaining on the non-FDIC computer, depending on how Employee-C copied the files from the hard drive to the flash drive. Thus, Employee-C, or anyone else with access to her computer, may have been able to access sensitive FDIC information. The FDIC's CSIRT recommended that the FDIC examine the computer Employee-C used to transfer the data between the drives. The FDIC did not do so.<sup>42</sup>

On February 19, 2016, the DBMT learned additional information about Employee-C, including that:

- Employee-C had been on a performance improvement plan during her employment at the FDIC,
- Employee-C had not completed a requisite technical examination,
- Employee-C had been proposed for removal from her employment, and

---

<sup>41</sup> In her interview with OIG and FinCEN investigators on September 20, 2016, Employee-C told the investigators that she tried to destroy the external hard drive herself with a hammer, ran over it with her car, tried to damage it with a screwdriver, and eventually dropped it off at a hardware disposal company.

<sup>42</sup> At the time of her interview on September 20, 2016, Employee-C allowed the investigators to review and image her personal computer. Based on further investigation, we learned that 375 of the 388 FDIC files were found on Employee-C's personal computer. Employee-C indicated she did not know how that happened and suggested that the FDIC flash drive might have transferred some of those files to her personal computer.

- Employee-C had left the FDIC under a settlement agreement.

On March 7, 2016, about 3½ months after the FDIC discovered Employee-C had downloaded the information, the FDIC Legal Division sent a letter to Employee-C seeking confirmation of the destruction of the hard drive and details regarding such destruction. Further, the letter requested a statement from Employee-C acknowledging her obligation not to disclose confidential information, to turn over any confidential information she had, and to cooperate with the FDIC to appropriately deal with any such confidential information that may have been copied or disseminated.

On March 8, 2016, Employee-C provided a statement confirming that (1) she personally destroyed the hard drive after she transferred the files onto the personal USB that she turned over to the FDIC; (2) she took the hard drive to a hardware destruction facility; and (3) she did not receive a receipt for the destruction but she contacted the facility and was told that any devices dropped off during the time period when she dropped off her drive would have been destroyed. Employee-C stated that she did not have any other confidential information and that no other personal devices were used to transfer, store, or manipulate the confidential data (see Appendix V, page 130).<sup>43</sup> In subsequent email correspondence with the Legal Division, Employee-C additionally confirmed, on March 15, 2016, that she had not further copied or disseminated the sensitive PII.

#### FDIC Electronic Media Destruction

FDIC employees are instructed to use secure “EShred” consoles to dispose of electronic media, including thumb drives, when it is no longer required to perform his/her job duties. The consoles and destruction services are provided under a contract with Iron Mountain. Accordingly, it was inappropriate for Employee-C to utilize this hardware disposal company that was not authorized by the FDIC to possess, maintain, or destroy a device used for official FDIC business.

On March 18, 2016, the FDIC determined that the sensitive information downloaded by Employee-C contained the PII and sensitive information of 49,217 individuals and 15,446 businesses and entities, exceeding the OMB Memorandum M-16-03 threshold. On March 28, 2016, about 4½ months after the information was downloaded, the DBMT recommended that the incident was a breach and a “major incident” that needed to be reported to Congress pursuant to FISMA 2014.

On March 31, 2016, the DCP ISM contacted the hardware destruction facility and learned that it issued receipts and “Certificates of Destruction” for all disposals, although Employee-C had reported to the FDIC that she did not receive a receipt. The ISM further

---

<sup>43</sup> As previously mentioned, OIG and FinCEN investigators later discovered 375 of the 388 FDIC files on Employee-C’s personal computer.

noted that the company maintained a log of all disposals. The DBMT later learned that the hardware destruction facility would not maintain a record or receipt for such destructions, as it only keeps such a record if the customer purchases a premium data destruction service. That was not the case in this instance.

During a meeting on April 12, 2016, the DBMT determined the risk level of Incident C to be low due to a number of factors:

- Employee-C was cooperating with the FDIC in resolving the incident,
- Employee-C's integrity was not in doubt,
- The DBMT believed that she did not have malicious intent in taking the data,
- She confirmed that she did not misuse and had returned or destroyed the data, and
- The DBMT did not feel she had a reason to misuse the data.

The DBMT did not make a recommendation as to whether bank customers should be notified and/or offered credit monitoring services. The IRA for this incident included a partially completed risk analysis/impact assessment, which classified the overall sensitivity of the data as high; however, no risk level was assigned for overall probability of misuse, overall likelihood of harm, and overall ability of the FDIC to mitigate harm.

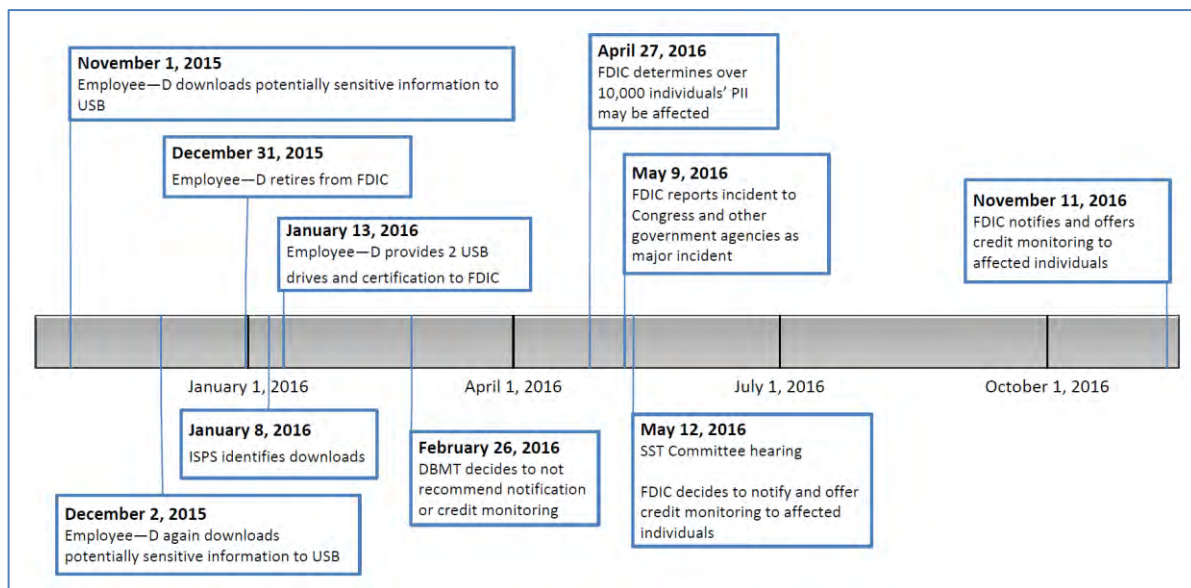
The FDIC ultimately reported Incident C, along with four other incidents, to Congress and other appropriate government agencies on May 9, 2016, approximately 6 months after the information was downloaded (see Appendix VI).

On May 12, 2016, after testifying before the SST Committee's Subcommittee on Oversight and after meeting with the FDIC Chairman, then-CIO Gross advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. The FDIC began notifying bank customers of the breach on December 13, 2016, more than 1 year after the information was downloaded, and offered credit monitoring services. Based on FDIC records, we understand that 33,969 individuals were offered credit monitoring services.<sup>44</sup>

---

<sup>44</sup> See footnote 37.

## F. Incident D



**Figure 9: Timeline for Incident D**

On January 8, 2016, the FDIC learned that Employee-D, a retiring RMS employee, had downloaded more than 2,000 files containing PII and sensitive information to two removable media devices on November 1 and December 2, 2015, before his last day in the office on December 11, 2015. The information included financial institution examination information, including SARs. Prior to his separation from the FDIC, Employee-D had signed the FDIC's standard Pre-Exit Clearance Form, certifying that he had not taken confidential information.

When first contacted in January 2016, Employee-D told his former supervisor that he intended to copy only training files and he asserted that he was not aware that the files contained embedded bank data. On January 13, 2016, Employee-D returned two USB drives, but based on the FDIC forensic analysis, the drives were blank.

When he returned the drives, Employee-D provided his former supervisor with a different explanation for his actions, indicating that he had downloaded the data to the USB drives as part of a monthly data backup process he used while working at the FDIC. Employee-D said that once he was contacted by his former supervisor, he reviewed the drives and found them to be blank. He then claimed that he had erased the data sometime between his last day in the office (December 11, 2015) and Christmas. Employee-D did not offer an explanation as to why he would erase the backup copies. Also, Employee-D presumably would have used an electronic device to erase the data from the USB drives.

The FDIC did not attempt to review Employee-D's personal computer.<sup>45</sup> At the FDIC's request, Employee-D signed a statement asserting the USB drives "were locked in a safe" at his home, that he had not disseminated any information, and that "the materials downloaded from [his] FDIC laptop to these USB storage devices were erased by [him] sometime in late December 2015" (see Appendix V, page 131).<sup>46</sup>

On February 26, 2016, the DBMT determined that the incident was a breach with a "low risk" of harm, and credit monitoring would not be offered "as a result of mitigating factors," which were not further described. The IRA for this incident contained a completed risk analysis/impact assessment, which classified the overall data sensitivity as high, the overall probability of misuse as low, the overall likelihood of harm as low, and the overall ability of the FDIC to mitigate harm as able to mitigate most harm.

On April 27, 2016, nearly 6 months since the first download of information by Employee-D, the FDIC determined that the PII or sensitive information of more than 10,000 individuals or entities was potentially involved in Incident D. On April 29, 2016, the count was finalized at 22,522 individuals and entities. The FDIC reported this incident to Congress and other appropriate government agencies pursuant to the requirements of FISMA 2014 on May 9, 2016, more than 6 months after the information was downloaded (see Appendix VI).

On May 12, 2016, after testifying before the SST Committee's Subcommittee on Oversight and meeting with the FDIC Chairman, then-CIO Gross advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. In its preparations for offering notification and credit monitoring, the FDIC determined that the final number of individuals to be offered notification and credit monitoring was 11,931.<sup>47</sup> The FDIC began notifying bank customers of the breach on November 11, 2016, over a year after the first download of information, and offered credit monitoring services.

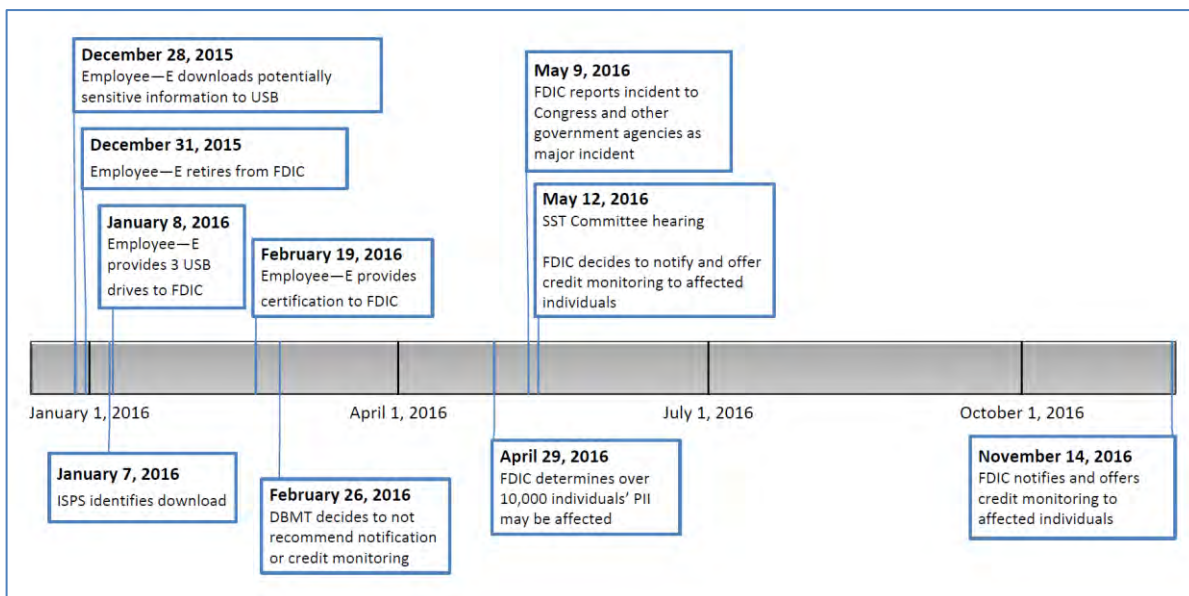
---

<sup>45</sup> In a later interview with OIG and FinCEN investigators on September 19, 2016, Employee-D did not consent to a search of his personal computer but insisted he no longer had any sensitive FDIC or banking information on his computer.

<sup>46</sup> In the subsequent interview with OIG and FinCEN investigators, Employee-D claimed that he first used his FDIC computer to wipe the drives, but he continued to state that he then wiped the drives again using his personal computer. He rationalized that the drives were already wiped of the FDIC data before he plugged them in to his personal computer.

<sup>47</sup> See footnote 37.

## G. Incident E



**Figure 10: Timeline for Incident E**

On January 7, 2016, the FDIC learned that Employee-E, a retiring RMS employee, had downloaded approximately 3,000 records containing bank customers' PII and other sensitive information, including SARs, to multiple removal media devices on December 28, 2015. Prior to his separation from the FDIC, Employee-E had signed the FDIC's standard Pre-Exit Clearance Form, certifying that he had not taken confidential information.

On January 8, 2016, Employee-E represented to his former FDIC supervisor that he was attempting to transfer personal files to the removable media devices, but the software he used did not allow him to select individual files. According to Employee-E, he initially tried to transfer the data to two FDIC-issued removable media drives, but when he was not able to do so, he transferred all of the data to a drive that he personally owned and later deleted the FDIC data from his personally-owned drive. Employee-E returned all three drives to his former FDIC supervisor on the same day, January 8, 2016.

Employee-E's former FDIC supervisor reviewed the drives and confirmed that no FDIC data were present on any of the drives, but the personally-owned drive contained some personal files. According to the IRA, on January 14, 2016, the RMS ISM informed the ISPS Incident Lead that the devices that Employee-E returned matched the devices flagged by the DLP tool and that the drives did not contain any FDIC data. Based on that information, the ISPS Incident Lead decided a DBMT was not needed at that time.

Employee-E returned a signed statement to the FDIC on February 19, 2016. Employee-E confirmed that he had not stored the data anywhere other than the drives; no one else had

access to the drives; the data had not been accessed, copied, downloaded, or disseminated in any way; and that he would further refrain from accessing or disclosing the information (see Appendix V, pages 132-133).

On February 26, 2016, the DBMT determined that Employee-E's personally-owned drive would be returned to him after the FDIC ensured that all FDIC data had been erased from the drive. The DBMT determined that this was a breach with a "low risk" of harm, and credit monitoring would not be offered "as a result of mitigating factors," which were not further described. The IRA for this incident contained a completed risk analysis/impact assessment, which classified the overall data sensitivity as high, the overall probability of misuse as low, the overall likelihood of harm as low, and the overall ability of the FDIC to mitigate harm as able to mitigate most harm.

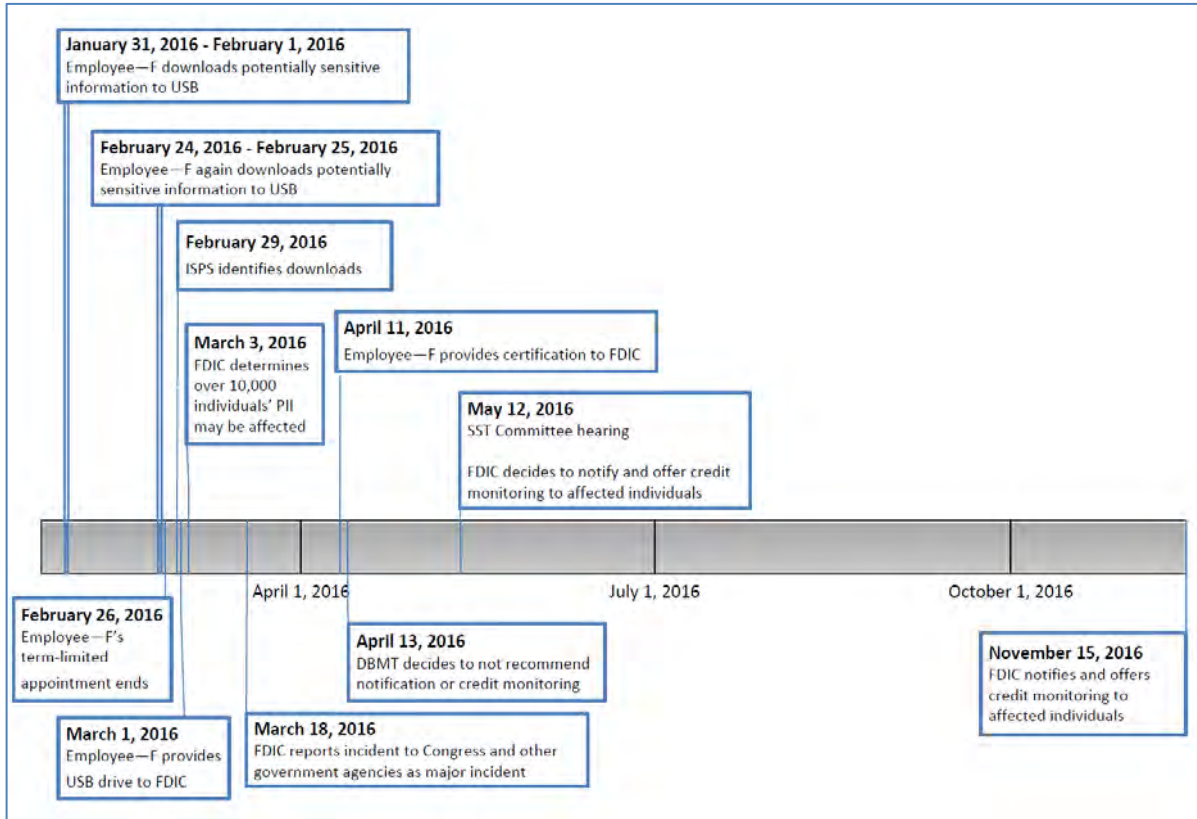
On April 29, 2016, about 4 months after the information was downloaded, the FDIC determined that the initial results of its review showed the PII or sensitive information of more than 10,000 individuals or entities was potentially compromised. As of May 3, 2016, the FDIC had determined that the PII and sensitive information of 18,668 individuals and 397 entities was compromised. The FDIC notified Congress and other appropriate government agencies of Incident E on May 9, 2016, over 4 months after the information was downloaded (see Appendix VI).

On May 12, 2016, after testifying before the SST Committee's Subcommittee on Oversight and after meeting with the FDIC Chairman, then-CIO Gross advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. In its preparations for offering notification and credit monitoring, the FDIC determined that the final number of individuals to be offered notification and credit monitoring was 11,417.<sup>48</sup> The FDIC began notifying bank customers of the data breach on November 14, 2016, nearly 11 months after the information was downloaded, and offered credit monitoring services.

---

<sup>48</sup> See footnote 37.

## H. Incident F



**Figure 11: Timeline for Incident F**

On February 29, 2016, the FDIC learned that Employee-F, a former DRR employee, had copied PII and sensitive information to a removable media device in January and February 2016. The device contained 112 files, including appraisals, compliance review reports, purchase and assumption agreements, and other loss-share related documents, that contained the PII of nearly 45,000 bank customers. Later that same day, DRR staff contacted Employee-F, and she returned the device that contained the data the following day, March 1, 2016. Prior to her separation from the FDIC, Employee-F had signed the FDIC's standard Pre-Exit Clearance Form, certifying that she had not taken confidential information.

According to the IRA for this incident, the DBMT "agreed that based on evidence provided, the download of FDIC information by the former employee was inadvertent. The former employee was copying a significant number of personal files (photographs, music) prior to



her departure from FDIC, and the FDIC files were inadvertently saved along with the personal data.”<sup>49</sup>

On March 18, 2016, almost 7 weeks after the first download of information, the FDIC notified Congress and other appropriate government agencies of the “major incident” pursuant to FISMA 2014 (see Appendix VI). On April 11, 2016, 10 weeks after the first download of information, Employee-F signed a statement agreeing that “[t]he Confidential Information was not accessed, copied, downloaded, or disseminated in any way” (see Appendix V, page 134).

On April 13, 2016, the DBMT determined the risk of harm of the breach to be “low” due to mitigating factors, including: the download was inadvertent; the employee was copying many personal files prior to her departure; she was a trusted employee, had no apparent malicious intent, and remained cooperative and responsive throughout the handling of the Incident; and there was no reason to believe she had done anything improper with the information. The IRA for this incident contained a completed risk analysis/impact assessment, which classified the overall data sensitivity as high, the overall probability of misuse as low, the overall likelihood of harm as low, and the overall ability of the FDIC to mitigate harm as able to mitigate most harm. Because they viewed the risk of harm to be low, the DBMT did not recommend notifying bank customers of the breach, nor did it recommend offering credit monitoring services.

Later, on May 12, 2016, after testifying before the SST Committee’s Subcommittee on Oversight and after meeting with the FDIC Chairman, then-CIO Gross advised his staff that credit monitoring would be offered to individuals whose sensitive information was involved in the breach. In its preparations for offering notification and credit monitoring, the FDIC determined that the final number of individuals to be offered notification and credit monitoring was 36,997.<sup>50</sup> The FDIC began notifying bank customers of the data breach on November 15, 2016, over 10 months after the first download of information, and offered credit monitoring services.

---

<sup>49</sup> In a subsequent interview with OIG and FinCEN investigators on September 20, 2016, Employee-F stated that she did not own a personal computer.

<sup>50</sup> See footnote 37.

## V. **OIG Findings and Analysis Regarding the FDIC’s Handling of Information Security Incidents and Breaches**

### A. **The FDIC Did Not Have Implementation Guidance and Procedures to Meet Statutory FISMA 2014 Deadlines**

The FISMA 2014 statute required that Federal agencies develop, document, and implement an agency-wide information security program that included, among other things, procedures for detecting, reporting, and responding to information security incidents. As noted earlier, FISMA 2014 introduced the concept of “major incident” and outlined a 7-day reporting requirement. Specifically, for “major incidents,” an agency had to notify and consult with appropriate Congressional Committees no later than 7 days after the date on which there was a reasonable basis to conclude that a “major incident” has occurred.<sup>51</sup> FISMA 2014 did not define the term “major incident” in the statute, but tasked OMB with developing guidance on what constitutes a “major incident.” OMB issued guidance relating to this term, in its Memorandum M-16-03, on October 30, 2015.

During the relevant timeframe of this Special Inquiry, OMB Memorandum M-16-03 provided that in determining when a data breach is a “major incident,” a Federal agency “shall consider” whether the incident involves data that is:

- “not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources;”
- “a high or medium functional impact to the mission of an agency;” or
- “the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either:
  - A specific threshold of number of records or users affected [10,000 or more records or 10,000 or more users affected]; or
  - any record of special importance [that is likely to result in a significant or demonstrable impact onto agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence].”

Our work showed that between the enactment of FISMA 2014 in December 2014 and the New York Incident in September 2015, which predated the issuance of OMB Memorandum

---

<sup>51</sup> This FISMA reporting requirement became effective the date the statute was enacted. The general rule is “that when a statute has no effective date, ‘absent a clear direction by Congress to the contrary, [it] takes effect on the date of its enactment.’” *Johnson v. U.S.*, 529 U.S. 694 (2000) (citing *Gozlon-Peretz v. U.S.*, 498 U.S. 395 (1991)).

M-16-03, the FDIC had not developed a comprehensive and thorough incident response plan, program, policies, or procedures to include reporting of such “major incidents” if or when they occurred. As a result, when confronted with the New York Incident, the FDIC was unprepared to promptly implement an effective and efficient process for reporting what was a serious breach of sensitive information.

Shortly after discovery of the New York Incident, in October 2015, attorneys in the FDIC Legal Division began discussing whether FISMA 2014 required the FDIC to notify Congress about the incident as a “major incident.” FDIC Legal Division management also internally debated whether to draft a legal opinion or interim guidance regarding the interpretation of FISMA 2014 and its reporting requirements. AGC Griffin and another Legal Division attorney perceived that FDIC upper management might not want a written legal opinion on this issue. In his interview for this Special Inquiry, AGC Griffin stated that “our sense at the time was that, it was a matter of high sensitivity on the 6<sup>th</sup> floor, very high sensitivity. And therefore, and because things aren’t cooked yet, don’t put it in writing.”

In late October 2015, after a series of discussions about whether or not to report the New York Incident to Congress, the Legal Division attorney began to draft interim guidance regarding what constituted a “major incident” under FISMA 2014. According to our interview for this Special Inquiry, the Legal Division attorney said that he was instructed by AGC Griffin not to type up the interim guidance and not to save it on an agency’s computer—rather, to handwrite it. Attorney work product is not typically handwritten; instead, it is usually drafted and saved in electronic form on the FDIC’s network. In the OIG interviews for this Special Inquiry, AGC Griffin acknowledged that the instruction was “inconvenient,” “troubling,” and “not the way one does business;” the Legal Division attorney described it as “strange;” and a Supervisory Counsel described it as “unusual.”

The Legal Division attorney believed that AGC Griffin was speaking on behalf of then-Deputy General Counsel Roberta McNerney (“then-DGC McNerney”).<sup>52</sup> AGC Griffin confirmed that then-DGC McNerney had given the instruction. The Legal Division attorney said that “it is the first time in decades that I was ever directed to do any legal work that required scratching it out by hand on a yellow legal pad.” The Legal Division attorney’s supervisor, the Supervisory Counsel, also recalled a similar instruction being relayed – “the instruction was to first put it on paper, and I think [AGC Griffin] gave instruction to [the Legal Division attorney] to start long hand-writing it as opposed to . . . saving it to [a] file.”

---

<sup>52</sup> Ms. McNerney retired from the FDIC on September 30, 2017, and is therefore referred to throughout this report as “then-DGC McNerney” or “former DGC McNerney.”

Then, on October 27, 2015, the Legal Division attorney made a contemporaneous note that he was instructed by AGC Griffin that pursuant to instructions from then-DGC McNerney, he could type, but not save to the FDIC's computer system, his handwritten draft, because "the sixth fl. may not want." It is not precisely clear to whom she was referring, but the "Sixth Floor" is generally understood to mean the Office of the Chairman. AGC Griffin recalled that then-DGC McNerney provided the instruction to the Supervisory Counsel, the Legal Division attorney, and him on a conference call. According to the Legal Division attorney, once the text of the draft guidance was typed, a hard copy was printed for limited distribution to the Supervisory Counsel and AGC Griffin later on October 27.

The next day, October 28, 2015, the Legal Division attorney made a contemporaneous note during a conference call that AGC Griffin reported that, according to then-DGC McNerney and then-OLA Director Eric Spitler,<sup>53</sup> "we can't share policy ideas until [the] 6<sup>th</sup> fl. is clear."

We interviewed both Chairman Gruenberg and COO Ryan and neither of them recalled expressing a view that the Executive Office must approve the provision of legal advice or guidance. Chairman Gruenberg further stated that he was not aware of anyone in the Chairman's Office driving the policy ideas related to "major incident" reporting.

According to our interview with the Legal Division attorney, AGC Griffin advised that then-DGC McNerney had asked for a copy of the interim guidance on FISMA 2014 on October 29, 2015. Apparently, then-DGC McNerney was looking for something else, because when AGC Griffin emailed the interim guidance, she replied by email:

As we discussed the day before yesterday and before, I asked you not to send around your suggested ideas for interim procedures (or anyone's ideas) because there are significant questions about what should be in the procedures and we need more input before drafts are ready to circulate.

Then-CISO Farrow similarly recounted in his OIG interview for this Special Inquiry that then-DGC McNerney told him, on or about November 16, 2015, that he should not put references to OMB Memorandum M-16-03 in email.

Then-DGC McNerney, in her interview for this Special Inquiry, stated that she neither instructed Legal Division staff to draft the interim implementation guidance regarding FISMA 2014 by hand, nor told staff to type but not save the draft implementation guidance. Then-DGC McNerney also denied instructing then-CISO Farrow not to put references to the OMB guidance in writing.

---

<sup>53</sup> Eric Spitler retired from his position as OLA Director on December 31, 2015. The FDIC Board of Directors approved the appointment of M. Andy Jiminez as the new OLA Director at that time.

Further, then-DGC McInerney explained in her interview that she told AGC Griffin in her email to him not to circulate ideas about interim procedures, because she had previously explained to him that she thought it was “a waste of resources to start drafting interim guidance for the seven-day reporting requirement.” Then-DGC McInerney believed that such work was premature, because, in her view, FISMA 2014’s reporting requirement for “major incidents” was not in effect until OMB issued guidance on what constituted a “major incident.”<sup>54</sup> She further stated that “there would need to be discussions about it, about what to put in it, how it would work, etc. So I basically, I did tell them not to send me any emails or anything more about it, because I just didn’t want it. To me, it was a complete waste of time to work on it.”

Meanwhile, in the absence of implementation guidance from the Legal Division, the CISO’s Office also began drafting an analysis of FISMA 2014’s reporting requirements. On October 20, 2015, a DIT employee began working with the Legal Division on implementation guidance regarding whether and how to report a “major incident” so that the Breach Guide could be updated. On October 29, 2015, the DIT employee wrote an email to himself in which he stated that “[w]e have identified a gap in policy in the Guide and need to fill in the gap; however, we are unable to receive any legal advice for what seems to be a rather routine matter.” He further stated that “[a]s I haven’t referenced the particular subject of what we’re not supposed to be talking about, I don’t consider this memorandum for record to violate [AGC Griffin’s] guidance not to create records.”

In an area as critical as information security, delayed or non-existent guidance hampers the ability of the FDIC to effectively address information security incidents and comply with applicable laws. Irrespective of the discussions or instructions within the Legal Division, the CIOO, ISPS, and other divisions within the FDIC did not have timely interim guidance on how to implement the provisions of FISMA 2014 and whether and how to report a “major incident.” Moreover, although then-DGC McInerney stated that her intention was to communicate to staff that it was too early to begin drafting interim guidance, her staff interpreted the message to be focused on not creating electronic records relating to formulating positions and implementation guidance for “major incident” reporting.

OMB published its Memorandum M-16-03 on October 30, 2015. On November 18, 2015, the Legal Division issued an opinion on the applicability of OMB Memorandum M-16-03. The opinion was signed by the Legal Division attorney through the Supervisory Counsel. The opinion indicated that OMB Memorandum M-16-03 is “generally applicable” to the FDIC. It also noted that to the extent the memorandum established policies and practices

---

<sup>54</sup> As noted earlier in footnote 51, the FISMA 2014 reporting requirement for “major incidents” was in effect upon enactment of the statute.

that were within OMB's authority under FISMA, OMB Memorandum M-16-03 imposes legally binding obligations on the FDIC. The opinion also noted that OMB's approach for analyzing "major incidents" appeared to be legally sound. The opinion did not provide clarity regarding how the FDIC should implement the guidance, but did describe 10,000 records as a "threshold number" for reporting incidents to Congress.

On February 19, 2016, in the course of our audit of *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*, we issued a memorandum to then-CIO Gross entitled *Information Security Incident Warranting Congressional Reporting*. The OIG memorandum stated that reasonable grounds existed to designate the Florida Incident as major as of December 2, 2015, and, as such, the incident should have been reported to Congress. We noted in the memorandum that the CIO articulated several factors that, in his view, mitigated the potential risk or impact of the incident. We stated that OMB Memorandum M-16-03 does not provide for the application of such factors in determining whether an incident is major.

When interviewed by our office, the Legal Division attorney concurred with the conclusions in the OIG's memorandum dated February 19, 2016, and he further stated that he felt that "[t]he agency should've reported [the Florida Incident] a long time ago" probably on or around December 9, 2015.

In his response to the FDIC OIG memorandum, on February 24, 2016, then-CIO Gross stated that "[i]n evaluating whether or not to classify an incident as 'major' using the M-16-03 guidance, mitigating factors should be taken into consideration . . . After reviewing your memorandum, carefully considering the analysis presented, and out of an abundance of caution, it is agreed the FDIC will immediately notify the appropriate congressional committees."

Although the CIO agreed to notify Congress of the Florida Incident, there still appeared to be an absence of direction from the Legal Division on implementing the FISMA 2014 and OMB Memorandum M-16-03 reporting requirements. On April 6, 2016, the DIT employee e-mailed the Supervisory Counsel about the 30-day reporting requirement in FISMA 2014:

I was told that the Legal Division's position is that the FDIC is not required to notify Congress about every data breach under the "30 day notification" until such time as OMB issues further guidance . . . on how to accomplish the notification and any other details OMB may further stipulate . . . could you please confirm that I have correctly stated Legal's position regarding the 30 day notification?

In an e-mail to himself on April 22, 2016, the DIT employee wrote:

After [the Supervisory Counsel] received my email, he called me to address my concern (no email reply). My take away was that the 30 day requirement should be there, but there appears to be some hang-ups within Legal ([AGC Griffin]? [then-DGC McInerney]?) that are interested in finding ways to postpone Congressional notifications.

Since the incident back in September 2015 and then again with the Florida incident, it has been extremely difficult to get any written feedback from [the Supervisory Counsel's] Opinions Unit or from [AGC] Griffin . . .

I'm not sure whether the actions over there are trying to cover-up the Florida incident or are trying to misconstrue what is really pretty straightforward reporting [requirements] in FISMA 2014 and OMB M-16-03.

Subsequently, on June 20, 2016, in his response to questions-for-the-record ("QFR") from the SST Committee's Subcommittee on Oversight following the May 12, 2016, Subcommittee hearing, then-CIO Gross stated that he had received the FDIC OIG's February 19, 2016, memorandum and "understood the reasoning behind the OIG's interpretation of OMB Memorandum M-16-03 as it applied to the 'Florida breach'." He further stated that "I communicated to staff that we would use the OIG's interpretation going forward."

We also note that in his testimony before the SST Committee on July 14, 2016, Chairman Gruenberg stated that "[i]n retrospect, and in light of the OIG's report findings, we should not have considered what we believed to be mitigating factors when applying the OMB guidelines."

### **B. The FDIC Did Not Adhere to Existing Policies in Responding to the Florida Incident and That Approach Carried Over to Subsequent Incidents**

On December 2, 2015, ISPS determined that the Florida Incident involved the breach of more than 10,000 Social Security Numbers. As discussed earlier in this report, OMB Memorandum M-16-03 stated that an agency should consider a data breach a "major incident" when 10,000 or more records or individuals were affected.

However, the DBHG, at the time, did not yet contain procedures for making the determination that an incident was a "major incident." Therefore, the DBMT members believed that they did not have authority to recommend that the Florida Incident was a "major incident." Instead, they viewed their role as recommending that the Florida

Incident was a breach, with then-CIO Gross having the authority to accept or reject their recommendation. Accordingly, the DBMT met on November 25, 2015—the day before Thanksgiving—and recommended to the CIO that the Florida Incident be declared a breach.

Then-CIO Gross did not formally declare the Florida Incident a breach within the timeframe required under the DBHG. The DBHG required that the CIO review the DBMT's recommendation to declare it a breach within 8 hours of its determination and that he notify the Executive Office. Instead, after the DBMT meeting on November 25, 2015, then-CIO Gross immediately notified COO Ryan that the DBMT had recommended that the Florida Incident be classified as a "breach" and advised that his staff was preparing a report for the Executive Office. However, in an email to then-CIO Gross, COO Ryan, on leave for the Thanksgiving holiday, suggested "it would be a good idea if we discussed process on this issue prior to a final report. Given the holiday, can this wait until next week?" Then-CIO Gross agreed and stated that he would reach out to COO Ryan the following week to discuss.

After the holiday, then-CIO Gross provided daily updates to senior management at the FDIC, including COO Ryan. Then-CIO Gross also provided regular updates to then-DGC McInerney. In an email from Special Advisor Martin Henning ("Special Advisor Henning") to then-CIO Gross, such updates were in order "given the potential for Congressional reporting." Then-CIO Gross agreed and cited the "seriousness of the Florida incident" in an email to then-CISO Farrow, Director of RMS Doreen Eberley, Special Advisor Henning, and COO Ryan. At this time, the FDIC was attempting to retrieve the device from Employee-FL.

On December 2, 2015, shortly after the Thanksgiving holiday, FDIC staff confirmed that the Florida Incident involved more than 10,000 unique Social Security Numbers. At this time, the FDIC had not yet secured the return of the device. The ISPS Incident Lead, pursuant to his role as described in the DBHG, requested a DBMT meeting that same day to consider further actions. The DBHG stated that it was the DBMT's responsibility to consider and recommend further breach response and mitigation strategies, including determining the risk level of the breach and whether consumer notification was warranted for affected individuals and whether credit monitoring services were appropriate.

On December 3, 2015, then-CIO Gross emailed COO Ryan and then-DGC McInerney to inform them that he had decided to "forgo any additional DBMT meetings." In his interview for this Special Inquiry, then-CIO Gross stated that he likely believed the DBMT was continuing its analysis, and he did not believe that further meetings or updates were



necessary at that time. COO Ryan and then-DGC McInerney reported to us that they assumed the DBMT would continue to work.

On December 6, 2015, then-CIO Gross finalized a summary report that included a recommendation to the Chairman—without consulting or conferring with the DBMT—that stated the Florida Incident was not considered a “major incident.” The report did not contain any analysis supporting his decision. The next day, then-CIO Gross advised the ISPS Incident Lead that no further daily status reports or DBMT meetings would be required.

The CIO said that he had discussed his recommendation with COO Ryan, then-DGC McInerney, and a representative from OLA on or about December 7, 2015. According to then-CIO Gross, the participants considered and discussed the “major incident” guidance articulated in OMB Memorandum M-16-03.

The DBMT was not kept apprised of then-CIO Gross’ report, including his recommendation to the Chairman, or the related discussions. As a result, DBMT members and other FDIC staff with significant roles were not able to perform their functions, particularly with regard to the risk assessment and mitigation aspects of the breach response lifecycle, and did not know how to proceed.

Because the DBMT was not involved in, nor was notified of, this determination, its members neither understood the basis of the determination that the incident was not “major,” nor the reason why DBMT meetings were discontinued. Members of the DBMT continued to request that then-CIO Gross schedule another DBMT meeting, so that they could meet their responsibilities under the DBHG. This confusion was evident in the IRA, which contained information that was inconsistent with then-CIO Gross’ recommendation. The IRA indicated that RMS and ISPS personnel were still awaiting approval from Executive Management to declare the Florida Incident a breach during the 6-week period from December 14, 2015 through February 8, 2016—well after then-CIO Gross had recommended that the Florida Incident was considered to be a breach. The IRA also did not contain a completed risk analysis, which should have recorded and documented the risk determination for the Florida Incident.

In fact, the breach involved over 10,000 individuals, thereby exceeding one of OMB’s thresholds for considering a breach a “major incident,” and it concerned numerous Social Security Numbers. Pursuant to the DBHG, the risk of identity theft and the loss of Social Security Numbers could result in a finding of high risk that individuals might be harmed. Then-CIO Gross did not provide the DBMT an explanation for his determination that the

breach was not a “major incident,” even though the DBMT was suggesting that another meeting would be appropriate.

At the time that then-CIO Gross made his determination:

- The DBMT had not examined the device and could not have considered the risk that PII had been accessed or transferred to other devices by the employee.
- Employee-FL had not provided any written assurances that the data had not been accessed or transferred.
- Employee-FL’s attorney took possession of the device, which was not authorized and resulted in greater risk of unauthorized access to the information it contained. The DBMT had not considered the impact that this possession had on the risk level of the breach.
- The DBMT had not considered whether affected individuals should be notified that their PII had been breached.

Then-CIO Gross’ report to the Chairman dated December 6, 2015, appeared to influence the DBMT’s reviews of other incidents (Incidents A, B, D, E, and F). The DBMT determined that all of those incidents were “low risk” without fully considering and/or documenting the unique circumstances and risks they involved. We found that the IRA for Incident C, like the Florida Incident IRA, did not contain a completed, documented risk analysis/impact assessment, and there was insufficient information in the IRAs for Incidents A, B, D, E, and F to support the overall risk designation of low.

The importance of documenting risk determinations was highlighted for the FDIC in a 2013 review by the GAO, entitled *Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, regarding the extent to which the FDIC (and other agencies) had developed and implemented policies and procedures for responding to breaches of PII. The GAO made three recommendations directed to the FDIC to improve its responses to breaches of PII.

With respect to risk assessments, the GAO noted “unless these agencies document the reasoning behind their risk determinations, they may not be able to ensure they are assessing data breaches accurately and consistently.” The FDIC concurred with the GAO’s recommendations. Indeed, on November 22, 2013, the FDIC’s Acting CIO/CPO stated that the FDIC was “in the process of reviewing and revising our data breach guidance to make more explicit the need to conduct lessons learned for all applicable breaches.” In addition, the FDIC’s Acting CIO/CPO continued:

The FDIC is taking steps to review and strengthen the documentation process for breaches involving PII, including the supporting case file information, to facilitate greater understanding of the reasoning behind risk determinations and the timely offer of credit monitoring services to affected individuals, when applicable.

The GAO has since closed its three recommendations. Nevertheless, our Special Inquiry findings show that the actions taken were not effective in ensuring that the decisions and actions for the incidents we reviewed were properly documented.

As a result, the FDIC's ability to analyze, assess, replicate, or learn from these incident responses was limited. In addition, the FDIC did not benefit from the expertise of DBMT team members, information and risks unique to incidents were not properly and timely considered, and the need to notify individuals or provide them credit monitoring was not addressed thoroughly and with urgency. Further, the IRAs for the incidents we reviewed did not contain (1) complete and reliable information to protect the FDIC's business and legal interests or (2) a sufficient basis for the FDIC or an oversight body to conduct proper supervision of the incident response program.

### **C. The FDIC Placed Undue Reliance on Post-Employment Written Statements from Former Employees**

The FDIC's approach to investigating and assessing the risk of the 2015 and 2016 data breaches was not effective, in part because it relied on post-employment statements of former employees. The FDIC intended that the statements—in some cases prepared by FDIC officials—would help establish that the data was recovered and not disseminated, thus indicating that the risk of harm was mitigated. However, such statements could not substitute for a complete investigation of each incident. Moreover, the reliance that the FDIC placed in the post-employment statements was not prudent, because, as discussed below, they were no more credible than the Pre-Exit Clearance Forms and data questionnaires on which the employees denied taking data, and portions of the statements were contradicted by facts known to the FDIC.

#### **Excerpt of FDIC Pre-Exit Clearance Record for Employees**

I certify that:

All Corporation-owned property, equipment, and documents that were in my possession have been returned to the proper division/office or have been accounted for.

I have not removed any Confidential Information (as defined below) from FDIC premises ... I have returned to the FDIC all Confidential Information that I possessed (in whatever form it existed) and will not transmit or remove (in any format or in any medium) any Confidential Information to any address outside the FDIC between the signing of this certification and my departure from FDIC employment.

With respect to each of the former employees in all eight incidents, each falsely or inaccurately certified that they had not removed any confidential information from FDIC premises when they signed the Pre-Exit Clearance Form.

Departing employees were also required to complete the *Data Questionnaire for Departing/Transferring Employees/Contractors*. Each of the departing employees submitted the form, except the employee involved in the New York Incident. Employees A, B, D, and E, and the employee involved in the Florida Incident, each marked “No” on the questionnaire item that asks, “[a]re there other data locations off-site where FDIC documents might be held?” Employee-C also marked “No” for that item, but also noted on the questionnaire that she did have documents off-site on “[p]ortable electronic files, such as DVDs, CDs, [and] Thumb Drives.” The FDIC did not conduct follow-up inquiries regarding these responses.

Each of the former FDIC employees involved in the seven breaches (Employees FL, A, B, C, D, E, and F) also made written representations about the data after their breaches were detected. In some cases, the representations were contradicted by prior statements and/or a lack of truthfulness and cooperation exhibited by the former employees after the breaches were detected.

In two instances, assertions made in the post-employment statements were inconsistent with facts known to the FDIC and recorded in the IRAs. For example, Employee-A indicated, in his post-employment statement, that he had not copied the data to another device, while the IRA showed that he had.

In the case of Employee-E, the FDIC sent a letter prepared by the FDIC Legal Division that stated:

We realize that departing employees sometimes leave with Confidential Information inadvertently included among their personal information and possessions, and we appreciate your acting quickly to provide to us the equipment (described below a/k/a (“Device”)) containing the Confidential Information.

The IRA for Incident E showed that the FDIC was aware that Employee-E had claimed he downloaded FDIC data because he was not able to select and copy only his personal data. Regardless of the reason for doing so, Employee-E purposely downloaded the sensitive data. Further, by including the language quoted above, the FDIC provided Employee-E with a rationale that he could assert for downloading the data. We note that the FDIC was

aware at the time that this rationale was contrary to Employee-E's own statement as to why he had downloaded the data.

In response to the incidents and breaches discussed in this report, the FDIC's Legal Division researched potential actions that the FDIC could undertake to minimize breaches and discourage inappropriate behavior by current and former employees and contractors. The Legal Division officials identified several legal theories for seeking civil and administrative remedies against employees and contractors who violate FDIC cyber-security policies and procedures. The Legal Division determined that none of these theories was found to be compelling or straightforward in pursuing past cases. However, the Legal Division indicated that the FDIC had: (1) taken disciplinary steps, including proposed removal, against current employees for failure to safeguard sensitive government information (and certain contractor organizations had removed contractors from FDIC contracts); and (2) utilized the certification signed by separating personnel in obtaining cooperation from former employees or contractors.

#### **D. The FDIC's Notifications to Consumers Were Not Timely**

The DBHG stated that the FDIC aimed to provide notification to affected individuals and/or entities within 10 business days of completing the analysis of breach data. In the case of the seven incidents the FDIC determined to be breaches, (the Florida Incident and Incidents A, B, C, D, E, and F), it took between 181 and 264 business days from the date the FDIC discovered the information was downloaded until it began sending notification letters to affected individuals and offering credit monitoring services. These delays were the culmination of lengthy timeframes for investigating the breaches, deciding whether notification was warranted, and ultimately executing the notifications. Such delays in customer notification did not permit affected individuals to take steps on their own to mitigate the risks caused by the breaches.

OMB Memorandum M-17-12 provided that:

Once the SAOP assessed the risk of harm to individuals potentially affected by a breach, the SAOP, in coordination with the breach response team when applicable, should consider how best to mitigate the identified risks. The SAOP, in coordination with the breach response team when applicable, was responsible for advising the head of the agency on whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach.

The SAOP should determine and document the actions that the agency would take to mitigate the risk of harm. These actions could include:

- Countermeasures, such as expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII;
- Guidance, such as how individuals may obtain a free credit report and whether they should consider closing certain accounts; and
- Services, such as identity and/or credit monitoring.

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP should consider what guidance to provide to those individuals about how they may mitigate their own risk of harm. There are several steps that individuals can take to mitigate their own risk of harm resulting from a breach, including setting up fraud alerts or credit freezes, changing or closing accounts, and taking advantage of services made available by the FTC.<sup>55</sup>

The SAOP should also determine if there are services the agency could provide, such as credit monitoring, identity monitoring, full-service identity counseling and remediation services, or identity theft insurance. Choosing not to provide services is a decision separate from the decision to provide notification, and there may be circumstances where potentially affected individuals are notified but not provided such services.

The Breach Guide recognized that a critical function of the DBMT was determining appropriate actions to mitigate harm, and recommending whether to notify affected individuals and/or provide credit monitoring. Neither our review of documentation, nor interviews of those involved in the breach response process (including members of the DBMT), provided an indication that customer notice and credit monitoring were evaluated as separate decisions.

As noted above, the work of the DBMT was effectively suspended after then-CIO Gross determined that the Florida Incident was not a “major incident.” As a result, the DBMT did not consider, in a timely manner, the risk of harm to the more than 10,000 individuals initially estimated to have been impacted by the incident. Further, because the analysis supporting then-CIO Gross’ “major incident” determination was not documented, it was not clear how he reached this conclusion. The IRA for the Florida Incident reflected that about 4 months later, on April 4, 2016, the DBMT declared the incident was low risk and recommended that consumers not be notified or offered credit monitoring services.

Similarly, for five incidents determined to be breaches (Incidents A, B, D, E, and F), it took the FDIC between 1½ and 3½ months from the date on which it learned of the download to

---

<sup>55</sup> The FTC provides information for consumers impacted by identity theft at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft> and <https://www.identitytheft.gov/>.

make a determination regarding whether notification and credit monitoring were necessary. For Incident C, the DBMT still had not made a determination about customer notification and credit monitoring services at the time that Chairman Gruenberg declared they would be offered (May 12, 2016).

At the SST Committee's Subcommittee on Oversight hearing on May 12, 2016, then-CIO Gross stated that the FDIC had decided not to offer credit monitoring services to consumers affected by these breaches; however, as previously discussed, that decision was reversed later the same day. Based on our work related to this Special Inquiry, we did not locate documentation for the reasons behind this decision.

As noted earlier in this report, the OIG issued an audit report entitled *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information*. This audit performed in-depth analysis of the adequacy of the FDIC's process for (1) evaluating the risk of harm to individuals potentially affected by a breach and (2) notifying and providing services to those individuals, when appropriate. OIG auditors interviewed then-CIO Gross, Chairman Gruenberg, and COO Ryan regarding the decision to ultimately provide notification and credit monitoring to individuals potentially affected by the breaches. According to then-CIO Gross, the FDIC changed its position because the original decisions not to notify potentially affected individuals were inconsistent with "major incident" designations, and because of public visibility and the Congressional hearing. Then-CIO Gross also indicated that the decision to provide notification and credit monitoring would have required the Chairman's approval.

Chairman Gruenberg stated that then-CIO Gross' recollection of events is generally consistent with his own. He stated that he recalled having an informal meeting after the hearing. Based on advice he received from the COO, CIO, OLA Director, and Deputy to the Chairman for Communications at the meeting, he decided that the FDIC should provide notification to potentially affected individuals and credit monitoring services. Later that same evening, then-CIO Gross advised his staff that credit monitoring services would be offered to all bank customers whose PII had been compromised.

Notably, the FDIC did not begin delivering notices to potentially affected individuals for at least another 6 months, in November and December 2016.

#### **E. Designating the CIO and SAOP/CPO Roles Within the Same Position Warrants Further Evaluation**

As noted earlier in our report, the FDIC designated the CIO as CPO in response to statutory requirements and associated OMB guidance. The CIO/CPO also serves as the FDIC's SAOP.

Guidance issued subsequent to these data breaches in 2015 and 2016 suggests that the FDIC may wish to reconsider its designation for the CIO as SAOP/CPO.

On September 15, 2016, OMB issued revised guidance regarding the role of the SAOP. OMB Memorandum M-16-24 stated that each agency must have an agency-wide program led by an SAOP for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission. For example, "[i]n this role, the SAOP shall ensure that the agency considers and addresses the privacy implications of all agency regulations and policies, and shall lead the agency's evaluation of the privacy implications of legislative proposals, congressional testimony, and other materials pursuant to OMB Circular No. A-19."<sup>56</sup>

Notably, OMB Memorandum M-16-24 stated that:

[A]gencies should recognize that privacy and security are independent and separate disciplines. While privacy and security require coordination, they often raise distinct concerns and require different expertise and different approaches. The distinction between privacy and security is one of the reasons that the Executive Branch has established a Federal Privacy Council independent from the Chief Information Officers Council.

In response, on November 9, 2016, the FDIC's CIO/CPO submitted a Memorandum to the Chairman regarding an internal evaluation of the FDIC Privacy Program. In particular, this evaluation memorandum considered the "Designation of the Senior Agency Official for Privacy," particularly in light of the position, expertise, and authority. The CIO/CPO's evaluation memorandum concluded that the FDIC Privacy Program—with the CIO serving as SAOP/CPO—was compliant with existing law and OMB guidance.

Later, on January 3, 2017, OMB issued follow-up guidance regarding additional requirements for the agencies and the SAOP with respect to preparing for and responding to breaches of PII. The OMB guidance also expanded the SAOP's direct responsibility, as distinct from the CIO's role, for preparing for and responding to breaches. The OMB guidance provided a list of individuals that should be on the agency's breach response team and listed the SAOP and CIO separately.

---

<sup>56</sup> The SAOP must ensure statutory compliance with the relevant authorities, including the Privacy Act of 1974; the Paperwork Reduction Act of 1995; the E-Government Act of 2002; the Health Insurance Portability and Accountability Act of 1996; OMB Circular A-130; Privacy Act Implementation: Guidelines and Responsibilities; OMB Circular A-108; OMB's Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988; and OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.



In light of the updated requirements and responsibilities for the SAOP/CPO, the FDIC may wish to reconsider and make more distinct its designated roles for the CIO and SAOP/CPO, taking into account the following factors:

- The perspectives of the SAOP/CPO are different from those of the CIO. The CIO has responsibility for maintaining a broad, strategic orientation focused on enterprise issues and concerns and protecting the agency's IT resources. These issues relate to the management of the FDIC's IT systems, enterprise architecture for its IT systems, governance of the IT programs and resources, acquisition of IT hardware, IT personnel, information security, and continuity of operations. By contrast, the CPO's (and SAOP's) role is oriented towards the privacy of individuals, including FDIC programs, policies, and procedures that affect bank customers and those that impact its own FDIC personnel, and reducing the risk of harm to potentially affected individuals in the event of a breach.
- The SAOP/CPO has responsibility for privacy issues and concerns that extend beyond IT issues. For example, the SAOP/CPO has responsibilities for the privacy implications related to FDIC materials that are not in electronic form. In addition, the SAOP/CPO is responsible for the privacy implications of internal FDIC programs that might affect FDIC personnel. The SAOP/CPO is further responsible for the privacy implications of disclosures of information outside of the FDIC, and this individual may need to make decisions about the laws and regulations governing privacy law, discovery productions in litigation, Freedom of Information Act requests, and other disclosure laws and regulations.

We view this matter as one of continuing interest that warrants further consideration.

#### **F. The FDIC Did Not Timely Notify the Financial Crimes Enforcement Network**

On November 23, 2010, FinCEN issued an advisory to regulatory and law enforcement agencies, self-regulatory organizations, and financial institutions to reinforce and reiterate the requirement to preserve the confidentiality of information contained within Suspicious Activity Reports. The advisory stated, among other things, that if a regulatory or law enforcement entity became aware of an unauthorized disclosure of a SAR, the agency should notify FinCEN's Office of Chief Counsel immediately.

As noted in FinCEN Advisory FIN-2012-A002, *SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions*, dated March 2, 2012:

The unauthorized disclosure of SARs could undermine ongoing and future investigations by tipping off suspects, deterring financial institutions from

filing SARs, and threatening the safety and security of institutions and individuals who file such reports. Such disclosure of SARs compromises the essential role SARs play in protecting our financial system and in preventing and detecting financial crimes and terrorist financing. The success of the SAR reporting system depends upon the financial sector's confidence that these reports will be appropriately protected.

On April 12, 2016, the OIG informed the FDIC that it should notify FinCEN to determine its breach-related reporting requirements in connection with the Florida Incident. The FDIC initially contacted FinCEN on May 4, 2016, and provided FinCEN with specific data regarding the breach during subsequent communications.

Three other incidents discussed above in this Special Inquiry report (Incidents B, D, and E) also involved an unauthorized disclosure of SAR information. FDIC records we reviewed did not indicate that SAR information was involved in Incidents A, C, and F; however, FinCEN's

investigative reports do indicate that BSA material was involved in these incidents. Incidents B, D, and E were detected by the FDIC between November 2015 and January 2016. The FDIC reported these breaches to FinCEN on May 18, 2016—approximately 4 to 6 months after the incidents were identified.

FinCEN opened cases on Incidents A, B, C, D, E, and F. In reporting its results, FinCEN indicated that the information was not further disseminated or misused and there was no criminal intent in the unauthorized download. FinCEN also determined that the electronic devices used to store the unauthorized data were returned to the FDIC for destruction in all but one case (Incident C). In that case, Employee-C asserted that she had destroyed the FDIC's device and returned the personal external drive on which she had saved the unauthorized data to the FDIC. FinCEN closed all six cases.

#### Suspicious Activity Reports

Federal law (31 U.S.C. 5318(g)(2)) prohibits the notification of any person that is involved in the activity being reported on a SAR that the activity has been reported. FinCEN guidance explains that this prohibition effectively precludes the disclosure of a SAR or the fact that a SAR has been filed to anyone.

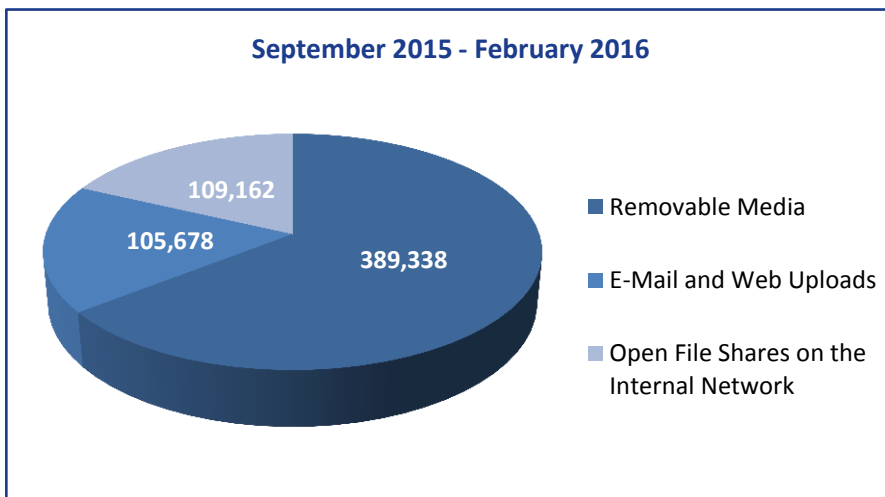
### **G. The FDIC Lacked Procedures and Resources to Promptly Review Information Generated by the Data Loss Prevention Tool**

The DLP tool detected each of the incidents discussed in this report and is a useful resource to assist the FDIC in safeguarding information. The DLP tool captures potential vulnerabilities, but absent resources, the information it provides cannot be timely reviewed and used to protect FDIC data. Each event flagged by the DLP tool required a manual review to determine whether it was a false positive, such as an employee downloading

business information to a flash drive for a legitimate business purpose (when that practice was still permitted at the FDIC). However, as the OIG reported in its audit entitled *The FDIC’s Process for Identifying and Reporting Major Information Security Incidents*, the FDIC had insufficient staffing to monitor the information provided by the DLP tool. At the time of the incidents, only one ISPS member was reviewing the potential hits generated by the DLP tool.

At the time of the incidents, from September 2015 to February 2016, the DLP tool flagged 604,178 potential security violations (events). The chart below illustrates the types of events involved.

**Figure 12: Security Violations Detected**



With respect to the incidents reviewed as part of this Special Inquiry, responsible FDIC staff did not discover the downloads of information until 4 to 68 days after the DLP tool had detected them. In each case, the FDIC had not become aware of the download until after the former employee had already separated.

The large volume of potential security violations identified by the DLP tool, together with limited resources devoted to reviewing these potential violations, hindered meaningful analysis of the information and the FDIC’s ability to identify all incidents, including “major incidents.” Moreover, the FDIC’s practice at the time of these incidents was to review information for departing employees after their departure. Accordingly, the FDIC was not able to review the information in a timely manner, and it missed opportunities to prevent the incidents. Our previous audit report entitled *The FDIC’s Process for Identifying and Reporting Major Information Security Incidents* recommended that the FDIC review its implementation and use of the DLP tool to determine how the tool can be better leveraged

to safeguard sensitive FDIC information. The FDIC has taken steps to implement this recommendation, and it is now closed.

The OIG's evaluation of *Controls over Separating Personnel's Access to Sensitive Information* also found that the FDIC's current pre-exit clearance guidance for FDIC employees or contractors did not include using the DLP tool, despite its use for the past year to monitor the network activity of separating employees. After the breaches by separating employees that occurred in late 2015 and early 2016, ISPS began receiving notice of employee separations and was informed by the Legal Division when employees of interest were scheduled to separate from the FDIC.<sup>57</sup> However, the FDIC was not conducting such reviews for contractors until after they separated. Our evaluation report included two recommendations to address these findings and the FDIC has indicated that related corrective actions are due to be implemented throughout 2018.

## H. Recommendations

Our Special Inquiry shows that the FDIC had not taken sufficient steps to ensure that it had a comprehensive incident response program and plan. Importantly, it did not have timely legal guidance on whether and how FISMA 2014 and OMB implementing guidance on reporting incidents applied to the FDIC. The FDIC must ensure that risk assessments and decisions associated with incidents are clearly documented, contrary to what we found for the incidents addressed in this Special Inquiry. Absent such documentation, the FDIC:

- could not ensure consistent treatment of incidents;
- did not have precedent to evaluate future misconduct in a consistent manner and take appropriate action; and
- lacked sufficient information for the agency or an oversight body to conduct proper supervision or control over the program.

The program should be designed to address these findings and ensure compliance with reporting requirements and applicable implementation guidance, including urgent reporting of "major incidents" to Congress and other government agencies, as required. Once established, the FDIC should put measures in place to assure adherence to incident response procedures. Such measures should include tabletop exercises, as prescribed by OMB Memorandum M-17-12, which serve to test the breach response plan and help

---

<sup>57</sup> Employees of interest include: (1) employees subject to removal actions; (2) employees retiring in less than 2 weeks because they would not appear on the Division of Administration-Human Resources Branch personnel actions email; and (3) employees involved in suspicious information security practices such as having a family member send an email that contains sensitive information from the employee's home computer to their work email address.

ensure all those involved in breach response are familiar with the plan and understand their specific roles.

Throughout and subsequent to our Special Inquiry, the FDIC took steps to address prior recommendations pertaining to incident and breach response. Notably, as discussed earlier, the FDIC issued revised incident and breach response guidance. To further improve its incident response program, we recommend that the FDIC:

1. Ensure that revised incident and breach response guidance clearly defines the roles and responsibilities for each participant in the incident response lifecycle, including the DBMT members, Chief Information Security Officer, Chief Information Officer, Chief Privacy Officer/Senior Agency Official for Privacy, Chief Operating Officer, and Chairman, and the participants are advised of and trained in those roles.
2. Establish procedures for identifying, tracking, and providing guidance on the applicability and implementation of new statutory requirements and government-wide guidance.
3. Establish procedures that describe the manner in which legal opinions are developed, deliberated, and provided to divisions and offices and that are consistent with legal, regulatory, and/or operational requirements for records management.
4. Emphasize that consumer notification of a breach should be considered separate from the decision to offer credit monitoring services.
5. Establish responsibility and adhere to established timeframes for reporting incidents to FinCEN where SAR information has been compromised.
6. Ensure that all key officials involved in incident responses are required to participate in periodic tabletop exercises to test the incident response plan.
7. Ensure that annual reviews established in the Breach Response Plan include steps designed to confirm that it has been consistently followed in responding to incidents during the past year.

Once faced with determining the risk associated with the data breaches and recovering the data involved, we determined that the FDIC's approach to investigating and assessing the risk of the data breaches was not effective. The manner in which the FDIC prepared the post-employment statements did not fully protect the FDIC's interests, including holding

former employees and contractors accountable for their actions. Accordingly, we recommend that the FDIC:

8. Define and determine the purpose of post-employment statements from former FDIC personnel and ensure the statements are consistently constructed to accomplish the defined purpose.
9. Develop guidance and training to ensure that employees and contractors are fully aware of the responsibility to return all FDIC equipment and documents and the prohibition against removing any sensitive information from FDIC premises before they depart, and understand the consequences—including available legal remedies—of providing false or inaccurate statements to the FDIC related to that responsibility.

## **VI. The FDIC's Reporting and Statements Regarding the Information Security Incidents and Breaches**

This Section of the Special Inquiry Report discusses the FDIC's reporting of the various information security incidents and breaches to Congress and the statements the FDIC made regarding them in its initial notifications to Congress and in subsequent interactions with Congress.

Congress derives its authority to conduct oversight of government agencies of the Executive Branch from its inherent legislative powers conferred by the U.S. Constitution. The Legislative Reorganization Acts of 1946 and 1970 codified this authority and authorized Congressional Committees to "review and study, on a continuing basis, the application, administration and execution" of laws. Congress, in its oversight capacity through its Committees, may conduct hearings and investigations and make requests for information of Executive agencies.

As discussed earlier, FISMA 2014 and related OMB implementing guidance required agencies to report security incidents to certain Committees of Congress.

### **A. Initial Notifications to Congress Under FISMA 2014**

#### **1. Reporting the New York Incident**

On three separate occasions in early November 2015, senior FDIC officials (including the CIO and CISO) convened to discuss reporting requirements under FISMA 2014, with respect to the New York Incident. The Chairman attended two of the meetings. As referenced

earlier, OMB Memorandum M-16-03 had recently been issued on October 30, 2015, and the FDIC was finalizing its annual submission to OMB pursuant to FISMA 2014.

According to our OIG interview with then-CISO Farrow for this Special Inquiry, he indicated that the meetings were focused on whether OMB Memorandum M-16-03 applied to the FDIC for the New York Incident, since the incident had occurred prior to the issuance of OMB Memorandum M-16-03.

Ultimately, the FDIC decided to include the New York Incident in its annual FISMA submission rather than reporting it separately. In his OIG interview for this Special Inquiry, Chairman Gruenberg noted that the annual FISMA submission would be the “natural vehicle” to report the incident, particularly given the closeness in time of the incident to the filing of the annual FISMA submission.

On November 13, 2015, the FDIC submitted the annual FISMA report, including a reference to the New York Incident. The transmittal for this report indicated that it had been “prepared following the guidance in OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*.” The transmittal letter also noted that none of the incidents in the annual report required “immediate Congressional notification.”<sup>58</sup>

The FDIC’s annual FISMA report (November 2015) contained the following language:

No incidents reported to US-CERT required immediate Congressional notification nor did they involve the loss of PII that would have required FDIC's provision of credit monitoring services. There were 20 breaches, 9 of which involved PII. For example, there were instances where sensitive financial institution information was mistakenly provided to a non-authorized party via an inadvertent email or via posting to an information exchange site in the wrong location. The unauthorized parties were contacted in each case to destroy the sensitive information. **In one instance sensitive business information regarding a limited number of large financial institutions was taken off premises by a departing employee. The sensitive information was recovered, and there is no evidence that the data was disseminated.** There were multiple instances where sensitive information was discovered in an internal location where access was too broad. Access control was corrected. [Emphasis added.]

---

<sup>58</sup> The FDIC reported 20 incidents in the annual FISMA report, including the New York Incident. The remaining 19 incidents did not include the incidents that we reviewed in this Special Inquiry, as all of the incidents in this report, except for the New York Incident, occurred after the FISMA 2015 reporting period.

During the course of our Special Inquiry, we learned that an earlier draft of this FISMA submission contained more details about the incident—namely that “[t]here was also an instance where a flash drive containing sensitive information regarding large financial institutions was taken off premises by a departing employee. The flash drive was recovered and there is no evidence that the data traveled beyond that flash drive.” These details about the flash drive were ultimately not included in the final FISMA report.

## **2. Reporting the Florida Incident**

With respect to the Florida Incident, while the DBMT considered the incident a breach, then-CIO Gross initially determined that it was not a “major incident” pursuant to OMB Memorandum M-16-03. He communicated his determination in a summary report that included a “Recommendation to the Chairman” on December 6, 2015: “after careful review of the Office of Management and Budget, Memorandum 16-03, dated October 30, 2015, the CIO does not recommend classification of this incident as a ‘Major Incident.’” Then-CIO Gross did not provide a rationale or an explanation for his conclusion in the report.

Based on the OIG interviews with COO Ryan and Chairman Gruenberg for this Special Inquiry, it appears that COO Ryan relayed then-CIO Gross’ recommendation about the reporting of the Florida Incident to the Chairman, and the Chairman accepted it. Then-CIO Gross, in his interview for this Special Inquiry, said that he was not aware, at the time, that the Chairman had accepted his recommendation.

Our Special Inquiry revealed that there had been some confusion within the FDIC about who was ultimately responsible for the determination as to whether an incident was considered a “major incident” and thus needed to be reported to Congress within 7 days. Then-CIO Gross, in his interviews for our audit of *The FDIC’s Process for Identifying and Reporting Major Information Security Incidents*, said that he did not expect the Chairman to review or approve his recommendation regarding the Florida Incident. Then-CIO Gross believed that because he made a determination the Florida Incident was not a “major incident,” there would be no reason for the Chairman to review or approve this determination. Then-CIO Gross further stated that he expected the Chairman only to review the CIO’s determination if then-CIO Gross had recommended that the Florida Incident was a “major incident.”

According to the FISMA 2014 statute, OMB Memorandum M-16-03, and FDIC policy, the agency head—the FDIC Chairman, in this instance—would be required to submit the report to Congress and, therefore, it would be his responsibility to make such a determination.



Subsequently, on February 26, 2016, the FDIC changed its view and reported the Florida Incident to Congress as a “major incident,” in accordance with FISMA 2014 and OMB Memorandum M-16-03. As discussed previously, the OIG had notified then-CIO Gross, on February 19, 2016, that because the Florida Incident involved the breach of more than 10,000 records containing PII, it should have been reported to Congress as a “major incident” within the 7-day reporting period under FISMA 2014 and OMB Memorandum M-16-03. According to then-CIO Gross, after “carefully considering the analysis presented, and out of an abundance of caution,” the FDIC notified the Congressional Committees about the Florida Incident.

The FDIC notified the following Congressional Committees and government agencies: U.S. Senate Committee on Banking, Housing, and Urban Affairs; U.S. Senate Committee on Homeland Security and Governmental Affairs; U.S. Senate Committee on Commerce, Science, and Transportation; U.S. Senate Committee on the Judiciary; U.S. House of Representatives Committee on Financial Services; U.S. House of Representatives Committee on Science, Space, and Technology; U.S. House of Representatives Committee on Oversight and Government Reform; U.S. House of Representatives Committee on Homeland Security; U.S. House of Representatives Committee on the Judiciary; OMB; GAO; and the Department of Homeland Security.

### **3. Memoranda Supporting the Congressional Notifications**

As noted above, on February 26, 2016, the FDIC reported the Florida Incident to the Congressional Committees and government agencies. On March 18, 2016, the FDIC reported Incident F. The remaining five incidents (Incidents A, B, C, D, and E) were reported on May 9, 2016. In this notification, the FDIC stated that it had identified these five incidents as a result of its “retroactive review,” following the OIG’s Memorandum dated February 19, 2016.

For each of these incidents, the FDIC notification letter and memorandum conveyed the following information:

- The employee had access to the sensitive information for work purposes while employed by the FDIC.
- The evidence suggested that the sensitive information was downloaded by the former employee “inadvertently” and “without malicious intent.”
- The FDIC’s investigation did not indicate that any sensitive information had been disseminated or compromised beyond the former employee.

- The FDIC’s relationship with the former employee had not been “adversarial.” (This point was not included in the letter and memorandum associated with Incident C.)
- The individual signed (or indicated that they would be willing to sign) a statement attesting that the compromised information had not been further disseminated.
- The FDIC estimated the number of individuals whose personal information had been compromised by the breach.

**B. Subsequent FDIC Interactions with Congress Regarding the Information Security Incidents and Breaches**

In connection with these reports to Congress regarding the breaches, the FDIC had a number of interactions with Congressional Committees, including briefings, correspondence, and formal testimony:

- On April 8, 2016, the SST Committee requested documents regarding Incident F, all “major security breaches” involving FDIC information since 2009, documents and communications relating to FDIC policies and procedures regarding handling sensitive information on FDIC computers, and organization charts. The SST Committee also requested that the FDIC brief the Committee. The FDIC responded to this request on April 22, 2016 (see Appendix VII).
- On April 20, 2016, the SST Committee requested documents on the Florida Incident as well as documents and communications relating to OMB Memorandum M-16-03. On April 21, 2016, SST Committee staff requested modifications to the date range of the relevant documents by email. The FDIC responded to this request on May 4 and May 9, 2016 (see Appendix VIII).
- On April 21, 22, and 28, 2016, the FDIC conducted briefings for the staff of five Congressional Committees: the SST Committee; House Oversight and Government Reform Committee; Senate Banking Committee; Senate Commerce, Science, and Transportation Committee; and Senate Homeland Security and Governmental Affairs Committee.
- On May 6, 2016, SST Committee staff called the FDIC with questions about the document production.
- On May 12, 2016, then-CIO Gross testified before the SST Committee’s Subcommittee on Oversight on behalf of Chairman Gruenberg.
- On May 19, 2016, SST Committee Chairman Lamar Smith and Subcommittee on Oversight Chairman Barry Loudermilk questioned the completeness of the FDIC’s document production and characterized certain aspects of then-CIO Gross’ testimony as “false and misleading.” The two Chairmen requested that

FDIC Chairman Gruenberg review the testimony, provide further details, and clarify and/or amend it as necessary (see Appendix IX).

- On May 24, 2016, the SST Committee raised additional concerns about the FDIC's cybersecurity practices and then-CIO Gross' testimony, requested a preservation of pertinent documents, and requested transcribed interviews with nine FDIC employees (see Appendix XIV).
- On May 25, 2016, the FDIC requested clarification from the SST Committee for parameters of how it would like a search performed of the email vault in response to the April 8 and April 20 letters.
- On May 25, 2016, Chairman Gruenberg responded to the SST Committee and indicated that he would review the hearing transcript, once it became available (see Appendix IX).
- On May 27, 2016, the SST Committee's Subcommittee on Oversight provided then-CIO Gross with an opportunity to correct or clarify his testimony (see Appendix X).
- On June 7, 2016, FDIC General Counsel Charles Yi ("General Counsel Yi") responded to the SST Committee's letter of May 24, 2016, and provided documents that were responsive to the Committee's request. General Counsel Yi stated that the FDIC was continuing to review documents and would provide responsive materials on a rolling basis. He also stated that the FDIC had arranged the interviews with individuals requested by the SST Committee.
- On June 14, 2016, FDIC staff proposed parameters for performing the search of email requested by the SST Committee. The FDIC followed up this request with another request on June 22, 2016.
- On June 20, 2016, then-CIO Gross responded to the SST Committee's Subcommittee on Oversight, but he did not directly address the concern that his testimony was "false and misleading" (see Appendix X).
- On June 28, 2016, FDIC staff requested guidance from SST Committee staff on prioritizing documents for review and production.
- On July 14, 2016, Chairman Gruenberg testified before the SST Committee.
- On August 1, 2016, the SST Committee Chairman sent QFRs to the FDIC Chairman (see Appendix XI).
- On August 18, 2016, FDIC staff met with SST Committee staff to discuss aspects of the document production.
- On August 25, 2016, the FDIC responded to the QFRs (see Appendix XI).
- On September 23, 2016, the FDIC Chairman responded in writing to questions raised during the July 14, 2016, hearing (see Appendix XII).

## **1. Statements Made in Congressional Briefings (April 21, 22, and 28, 2016)**

On April 14, 2016, the FDIC offered briefings to the staff of seven Congressional Committees, and five Committees' staff accepted the offer. In advance of the first briefing scheduled with SST Committee staff, an OLA employee sent a meeting invitation by email, indicating that in speaking with Committee staff, the FDIC had been requested to brief staff on Incident F and "items similar in nature." The SST Committee letter of April 20, 2016, further reiterated that the Committee wanted to be briefed on the Florida Incident. OLA Director Jimenez confirmed to SST Committee staff that the FDIC would be prepared to brief on the Florida Incident.

The FDIC personnel involved in preparing for and conducting the briefings included then-DGC McNerney, AGC Griffin, Special Advisor Henning, DRR Deputy Director Pamela Farwig ("Deputy Director Farwig"), OLA Director Jimenez, and the OLA employee who set up the meetings with SST Committee staff. At the time of these briefings, the FDIC was investigating numerous potential "major incidents" and had already determined that three incidents reached the level of a "major incident": the Florida Incident, Incident C, and Incident F.

However, based upon our interview with Deputy Director Farwig for this Special Inquiry, we learned that the FDIC briefed the SST Committee staff on April 21, 2016, about only two such incidents—the Florida Incident and Incident F—and did not brief staff about Incident C. In that regard, we note that there was no representative from DCP at the briefing to speak specifically to the facts associated with Incident C, which involved a former DCP employee. An SST Committee staff member followed up on this apparent omission in an e-mail to the OLA employee. The e-mail cited a *Federal Times* article, which stated that there were additional "major incidents" to be reported: "[m]y recollection from the briefing is that FDIC said the two incidents from Oct. 2015 and Feb. 2016 were the ONLY two that they were aware of that rose to the level of a 'major breach.'" [Emphasis in original]

Subsequent briefings were held with the Senate Banking Committee (April 21), with the House Oversight and Government Reform Committee and Senate Commerce Committee (both on April 22), and with the Senate Homeland Security and Governmental Affairs Committee (April 28). The FDIC did not discuss Incident C at these briefings. At each of the briefings, FDIC staff explained that a review of other incidents was underway.

## **2. Congressional Testimony before the SST Committee’s Subcommittee on Oversight (May 12, 2016)**

On May 12, 2016, then-CIO Gross testified before the SST Committee’s Subcommittee on Oversight. In his written statement for his testimony, he stated that, for each of the seven reported “major incidents” (the Florida Incident and Incidents A, B, C, D, E, and F), the FDIC’s analysis indicated that:

- The employee had legitimate access to the sensitive data while at the FDIC;
- The downloading of PII was “inadvertent;”
- The data had been recovered from the former employee;
- There was no evidence that the former employee had disseminated the data beyond himself/herself;
- The former employee signed a statement indicating he/she had not disseminated the data; and
- The circumstances surrounding the employee’s departure from the FDIC were “non-adversarial.”

Then-CIO Gross provided similar information in his prepared oral remarks. During the hearing, in response to questions from members of Congress, then-CIO Gross reiterated that the departing FDIC employees inadvertently downloaded sensitive information, that the former employees were “non-adversarial,” and added that “[t]he individuals involved in these incidents were not computer proficient.” Then-CIO Gross further acknowledged that there was no way technologically to determine if the data had been copied and/or disseminated further, despite stating in his prepared remarks that there was no evidence of dissemination.

## **3. Follow-Up Letter from the SST Committee and the FDIC’s Response (May 19 and 25, 2016)**

On May 19, 2016, SST Committee Chairman Lamar Smith and Subcommittee on Oversight Chairman Barry Loudermilk sent a letter to the FDIC Chairman expressing concern that “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.”

The SST Committee letter outlined several areas of concern:

- Then-CIO Gross' testimony regarding the completeness of the FDIC's responses to the SST Committee's requests for documents and information.
- Then-CIO Gross' characterization of the Florida Incident at the hearing and in Congressional briefings in advance.
- Then-CIO Gross' description of the reported "major incidents" as "low risk" thus justifying a decision not to provide credit monitoring.
- The FDIC's continued failure to report "major incidents" to Congress within 7 days.

The SST Committee letter requested that the FDIC Chairman "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."

On May 25, 2016, the FDIC Chairman responded by stating that "[w]e look forward to reviewing the full, official hearing transcript so that additional responses may be provided as needed." Chairman Gruenberg's response further stated that "[i]n each [data breach], the information was recovered and there was no evidence of further dissemination or disclosure."

#### **4. Follow-Up Letter from SST Subcommittee on Oversight Hearing and the FDIC's Response (May 27 and June 20, 2016)**

On May 27, 2016, the SST Committee's Subcommittee on Oversight sent a letter to then-CIO Gross requesting that he review the transcript from the hearing of May 12, 2016, and provide responses to certain QFRs.

On June 20, 2016, then-CIO Gross responded by submitting his transcript corrections and responses to the QFRs. While then-CIO Gross provided factual clarifications to his testimony in three instances and grammatical corrections to specific lines in his testimony, his response did not address substantive issues. Then-CIO Gross' response did not address the issues raised by the SST Subcommittee on Oversight during his testimony, nor did it address the issues outlined in the SST Committee letter to the FDIC Chairman on May 19, 2016.

In his response of June 20, 2016, then-CIO Gross stated that the FDIC was "now in the process of offering credit monitoring services to the individuals at no cost to them to protect any individuals who were potentially affected, and to be responsive to the concerns raised by the members of the Committee." The FDIC did not begin notifying affected individuals about the breaches until November 11, 2016, nearly 5 months later.

## 5. Statements at Congressional Hearing before the SST Committee (July 14, 2016)

On July 14, 2016, the FDIC Chairman testified before the SST Committee regarding these breaches at the FDIC. During the hearing, Chairman Gruenberg reiterated in his response to questions from Members what he had stated in his letter dated May 25, 2016 – namely, that the FDIC had recovered all the information that had been compromised in each of the “major incidents.” Chairman Gruenberg indicated that, although it was not possible to state with certainty that no dissemination had occurred, the FDIC had not identified any such dissemination.

During the hearing, on July 14, 2016, Chairman Gruenberg stated that “[w]e are undertaking notifying and providing credit monitoring to all the individuals affected by those seven breaches.” As noted earlier, the FDIC did not begin notifying individuals affected by the breaches until November 11, 2016.

On August 1, 2016, the SST Committee Chairman sent QFRs from three Committee Members to Chairman Gruenberg, and Chairman Gruenberg sent his response on August 25, 2016. The response addressed such issues as FDIC encryption and two-factor authentication practices, the Corporation’s IT risk management strategy, use of red teaming to perform adversary simulations, the FDIC’s earlier APT incident, Digital Rights Management and DLP technologies, and actions to prevent data breaches related to removable media and FDIC employees.

On September 23, 2016, Chairman Gruenberg provided another response letter to the Chairman of the SST Committee, enclosing answers to questions raised during the hearing. Among other things, Chairman Gruenberg addressed issues relating to data classification, incidents flagged by the DLP tool since the ban on use of removable media, replacement of desktops for laptops, his awareness of instructions not to put things in writing, and individuals advising on the FDIC’s Insider Threat Program.

“In retrospect, and in light of the OIG’s report findings, we should not have considered what we believed to be mitigating factors when applying the OMB guidance. We also failed to provide adequate context when reporting to Congress on the Florida Incident and should have notified the potentially affected individuals when the notice to Congress was given in February.”

Source: [Transcript of Chairman Gruenberg’s Testimony on July 14, 2016](#)

## **VII. OIG Findings and Analysis Regarding the FDIC's Reporting and Statements**

### **A. The FDIC's Notifications to Congress under FISMA 2014 Were Not Timely**

As discussed earlier in our report, FISMA 2014 required that in the event of a "major incident," a Federal agency must notify and consult with, as appropriate, certain Committees of Congress not later than 7 days after the date on which there was a reasonable basis to conclude that the "major incident" occurred. In addition, agencies must, within a reasonable period of time after additional information about a "major incident" is discovered, provide further information to the Congressional Committees.

When it became apparent that certain incidents had potentially affected well over 10,000 individuals or records, the FDIC chose to delay reporting them to determine impact and report the incidents as a group rather than individually. This protracted approach resulted in the FDIC reporting the incidents to Congress beyond the initial 7-day notification requirement (with the exception of Incident A), and prevented Congress from taking timely steps to understand and address the associated risks.

Between October 23, 2015, and January 8, 2016, the FDIC discovered the Florida Incident and Incidents A, B, C, D, and E. In the case of Incident C, the FDIC estimated that the incident potentially involved 28,000 Social Security Numbers when it was discovered on December 10, 2015.

On February 19, 2016, the OIG notified the FDIC during the course of our audit of *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* that the Florida Incident should have been reported to Congress within 7 days as mandated by FISMA 2014 because the incident involved over 10,000 records involving PII. On February 26, 2016, the FDIC reported the Florida Incident to Congress, and according to then-CIO Gross, adopted the 10,000 PII record threshold for reporting "major incidents" to Congress. The FDIC could have also reported Incident C to Congress as a "major incident," given the FDIC had already estimated that it involved 28,000 Social Security Numbers. Instead, the CIO decided that the FDIC would review other incidents to determine if any should be reported to Congress and that the review would be completed by March 12, 2016.

On February 29, 2016, the FDIC became aware of Incident F. The FDIC subsequently reported Incident F to Congress on March 18, 2016. That same day (March 18, 2016), ISPS concluded that Incident C was a "major incident," because it involved the PII of 49,217 individuals and thus should be reported to Congress. On March 28, 2016, the DBMT, which



included then-CIO Gross, concluded that Incident C was a “major incident” and that it should be reported to Congress. At this point, over 100 days had passed since the FDIC originally estimated the incident exceeded the 10,000 PII-record threshold.

On March 29, 2016, then-CIO Gross reviewed and commented on a draft notification letter for Incident C. He asked the then-Acting CISO for a report on the status of the other incidents being tracked as potential “major incidents.” Then-CIO Gross stated that “[i]f we have additional [sic] that rises to this level, we should work to fully address the remaining so we do not piecemeal this issue.” The then-Acting CISO advised then-CIO Gross that the other incidents being tracked as possible “major incidents” were being actively handled by their respective ISMs.

By April 29, 2016, the FDIC determined that Incidents B, D, and E involved the PII of over 10,000 individuals. Nevertheless, rather than reporting those incidents at that time, then-CIO Gross stated that he was awaiting additional information on the other incidents but expected to report four additional “major incidents” to Congress. This approach was not consistent with the FISMA notification requirement, which called for notifying Congress when there is a reasonable basis to conclude a “major incident” had occurred.

On May 5, 2016, the FDIC determined that Incident A involved the PII or sensitive information of over 10,000 potentially affected individuals, although the count was still ongoing at that time. On May 9, 2016, following that determination, the FDIC reported Incidents A, B, C, D, and E to Congress.

Under the circumstances—a known statutory reporting requirement and a substantial number of potentially impacted individuals—the FDIC lacked urgency in completing the counts of such individuals. Specifically, the counts of potentially impacted individuals for Incidents A, B, D, and E were not finalized until 3½ to 7 months after the FDIC had discovered the downloads.

Finally, even after the FDIC determined that over 10,000 individuals were potentially affected, only Incident A was then reported within 7 days, as required. For Incidents B, D, and E, the FDIC reported the matter 10 to 12 days after that determination; whereas, for Incident C and the Florida Incident, the FDIC reported them 52 and 86 days afterward, respectively.

As noted earlier, the FDIC later learned that the initial estimated figures of potentially impacted individuals were incorrect. This resulted in the cumulative final number of individuals notified being substantially lower. The FDIC did not provide Congress with the additional updated information regarding the number of impacted individuals and the

actions it took to notify them and provide credit monitoring—despite the FISMA 2014 reporting requirement for the agency to provide an update on the response and remediation actions taken.

### **B. The FDIC's Characterization of the New York Incident Did Not Convey Its Seriousness**

The New York Incident was a serious information security incident at the FDIC. There was no disagreement among the FDIC personnel interviewed for this Special Inquiry about the severity of the incident, given the nature of the information compromised, i.e., sensitive resolution plans. The FDIC Chairman, in his interview for this Special Inquiry, indicated that he viewed the New York Incident as “clearly a significant, significant matter.”

Nevertheless, there were differing views as to the level of transparency around the FDIC's reporting of the New York Incident. As noted above, the FDIC reported the New York Incident as part of its annual FISMA submission, and not as a separate “major incident” within the 7-day reporting requirement under FISMA 2014.

Given the nature of the documents breached, we believe that the New York Incident should have been reported as a “major incident” under FISMA 2014 and OMB Memorandum M-16-03. The “living will” documents should have been considered “record[s] of special importance,” because they could result in a significant, demonstrable impact on the agency's mission, economic security, or public confidence.

The FDIC's 2015 FISMA report did not indicate that the “living will” information contained very sensitive business information about the nation's largest financial institutions. The information provided in the annual FISMA report also did not include important details about the event, such as the data was on a flash drive (making further unauthorized access and dissemination a greater risk) and that the employee involved posed a heightened security risk. In addition, the description of the incident was inserted between other examples of less serious security incidents. A reader of the submission could not have discerned the significance of the incident, and that some of the most sensitive documents at the FDIC had been compromised.

On November 16, 2015, Chairman Gruenberg, COO Ryan, then-DGC McInerney, General Counsel Yi, then-CIO Gross, then-CISO Farrow, Special Advisor Henning, then-Director of OLA Eric Spitler, current OLA Director Jiminez, and another FDIC attorney met to discuss the reporting of the New York Incident. In January 2016, then-CISO Farrow reported to the OIG that the “theme [of the November 16<sup>th</sup> meeting was] how not to report [the New York Incident] to Congress.” Then-CISO Farrow said that he suggested that the FDIC should

report the incident to Congress under the OMB Memorandum M-16-03 provisions because it would make the FDIC “look good” in that the FDIC had the capability to identify a breach and also said that his suggestion was rejected. Further, then-CISO Farrow believed that there was an effort to describe the New York Incident in the FISMA annual submission so that it would not be highlighted in the context of other incidents –“put in [the] middle of two benign instances” to “soft pedal” the reporting.<sup>59</sup>

In his subsequent OIG interview for this Special Inquiry in August 2016, Mr. Farrow again said that, at the meeting of November 16, 2015, he suggested the possibility that the FDIC notify Congress under the OMB Memorandum M-16-03 provisions because it would show that the FDIC had tools to identify incidents. Mr. Farrow thought it was the safer way to report, so there would be no question as to whether the FDIC reported the incident correctly. However, when asked whether there was reluctance to report things to Congress, Mr. Farrow said “there was a good amount of conversation about what the most appropriate way to report was, whether it would be in FISMA, Congress, or otherwise, but I don’t know if I can characterize anything as reluctance.”

To clarify Mr. Farrow’s earlier statements regarding the FDIC’s deliberations on reporting the incident, the OIG interviewed Mr. Farrow again in December 2016. At this time, Mr. Farrow confirmed that the “theme [of the meeting was] how not to report to Congress” and that the New York incident was “put in the middle of two benign instances” to “soft pedal” the reporting.

Others we interviewed did not recount such reluctance to report the New York Incident. Special Advisor Henning expressed the view that the description of the New York Incident should convey what happened, “without providing . . . more sensitive information than it needed to.”

We believe that the FDIC reporting the New York Incident in this manner made it less likely that the incident would receive attention and oversight.

---

<sup>59</sup> Notes taken by an FDIC attorney during an earlier (October 28, 2015) meeting where the New York Incident was discussed similarly reflected that then-Director of OLA Eric Spitler expressed a view that the New York Incident should be included in the FDIC’s annual FISMA report in a “summary,” so “no alarm” would be raised.

### **C. The FDIC's Statements Regarding the Breaches Included Characterizations That Were Overly Broad and Did Not Convey Potential Risks**

The FDIC made statements regarding the breaches and referenced mitigating factors in initial notifications to Congress in February, March, and May 2016; repeated similar characterizations in testimony in May and July 2016; and did not clarify or correct those characterizations in subsequent communications, notwithstanding challenges by Committee Members as to their accuracy. These characterizations were overly broad and did not convey the potential risks associated with the breaches.

The FDIC reported five of the breaches (Incidents A, B, C, D, and E) at one time, in notification letters on May 9, 2016, using virtually the same language to describe each one. The language was also very similar to that used when reporting the Florida Incident and Incident F. As a result, the notifications were sometimes inaccurate and imprecise, did not always convey the unique features of each breach, and tended to diminish the associated potential risks. When referencing the breaches in later testimony, some of these broad characterizations were again repeated.

#### **1. FDIC Statements That the Breaches Were Inadvertent**

As detailed above, the FDIC stated on multiple occasions that all of the breaches were “inadvertent.” In at least one case (Incident F), the downloading of sensitive information may have been inadvertent—that is, when the former employee was intending to download personal photos and instead copied sensitive FDIC information along with the photos. However, in other cases (Incidents A, D, and E), the employees had told their supervisors why they had purposely downloaded the information.

For example, according to the IRA for Incident A, when first contacted by his former supervisor about the DLP report, Employee-A said he had downloaded the data “in case he returned to the FDIC to work.” Also, Employee-D told his former FDIC supervisor that he downloaded the sensitive information as “part of his monthly backup process, which he performed because he did not trust the FDIC network backup process.”

In the case of Employee-E, he represented to his former FDIC supervisor that he was attempting to transfer personal files to the removable media devices, but the software he used did not allow him to select individual files. According to Employee-E, he initially tried to transfer the data to two FDIC-issued removable media drives, but when he was not able to do so, he transferred all of the data—files containing approximately 3,000 instances of sensitive information—to a drive that he personally owned and later deleted the FDIC data from the drive.

## **2. FDIC Statements That the Agency's Relationship with the Former Employees Was Non-Adversarial**

As described above, the FDIC made statements in its "major incident" notifications to Congress that the former employees (except Employee-C) had non-adversarial relationships with the FDIC. The FDIC had not defined the term "non-adversarial" in its policies or provided its meaning in communications regarding the incidents. Based on documentation we reviewed during this Special Inquiry, it appears the FDIC intended the term to mean that the former employees had cooperated in promptly returning the data and confirming they no longer possessed or had further disseminated the data.

For example, the IRA for Incident B indicated that Employee-B had mistakenly copied FDIC business sensitive information to his personally-owned hard drive and had been very cooperative in working with FDIC to ensure the timely and secure removal of the data from the drive. He also stated in his certification to the FDIC dated February 19, 2016, that he had not disseminated the information in any way. This documentation supports the FDIC's assertion that the relationship was non-adversarial.

In contrast with this incident, the former FDIC employee involved in the Florida Incident had three discussions with her FDIC supervisors, by telephone, during which she denied copying the information or owning a removable media device. During this time, Employee-FL refused to meet with FDIC staff. She eventually advised them that any further communication from the FDIC should be directed to the private legal counsel she had retained.

Further, the IRA for Incident A stated: "the employee admitted to copying the data, but was reticent about providing his personally-owned drive to FDIC so that the FDIC data could be securely removed." The IRA also indicated that Employee-A's supervisor had contacted the employee on eight occasions asking that the DLP-identified drive be returned to the FDIC so that the FDIC data could be removed. The DBMT agreed that the supervisor should facilitate a conference call with Employee-A to include the FDIC CISO and a representative of the Legal Division to take place the week of December 28, 2015. The IRA goes on to say that "[t]he CISO and Legal will cordially, but firmly, express the serious nature of the situation." Further, "[i]f the call is unsuccessful, Legal will prepare a letter to be sent to the employee shortly thereafter."

With respect to Incident C, the FDIC's "major incident" notification to Congress did not state that the relationship with Employee-C was non-adversarial as did the other notifications. However, then-CIO Gross indicated in his written statement for the Congressional hearing of May 12, 2016, that "in each case, the circumstances surrounding

the employee's departure from FDIC employment were non-adversarial." As noted previously, the DBMT, which included then-CIO Gross, was notified less than 3 months prior that Employee-C had been proposed for removal from the FDIC and left under a settlement agreement.

Further, our review determined that Employee-C was also not candid and forthright in her discussions with the FDIC. She initially denied copying FDIC files. When contacted by her former supervisor again, Employee-C admitted that she had accessed the hard drive to copy files to a USB drive after her supervisor called her for the purpose of confirming that she had not copied the files. Employee-C ultimately claimed that she destroyed the hard drive rather than return it to the FDIC. On February 25, 2016, AGC Griffin advised then-CIO Gross and others that there had been "less-than-full cooperation" between Employee-C and the FDIC.

### **3. FDIC Statements That the Sensitive Information Was Not Disseminated**

As noted previously, the FDIC addressed whether the data taken by the former employee had been further disseminated in each "major incident" notification letter to Congress. When reporting the Florida Incident in February 2016, the FDIC stated that its investigation did not indicate that any sensitive information had been disseminated and the individual was willing to sign a statement that information was not further disseminated. When first reporting Incident F in March 2016, the FDIC again stated that its investigation had not indicated that any sensitive information had been disseminated. The FDIC further noted that the Legal Division was coordinating the drafting of a statement so the employee could attest that there had not been any further dissemination of the underlying information.

For the five breaches reported on May 9, 2016, the FDIC represented that each individual involved had, in fact, signed or provided a statement indicating that the data had not been disseminated. In four of these cases (Incidents A, B, D, and E), the FDIC further indicated that the data had been in the employees' sole possession for the duration of the breach. The FDIC relied on these statements to support the contention that data had not been disseminated. Chairman Gruenberg also indicated in a response letter to the SST Committee on May 25, 2016, that in each of the six incidents reported to Congress following the Florida Incident, "there was no evidence of further dissemination or disclosure."

The FDIC, however, did not conduct independent forensic analysis on the devices that were returned that was sufficient to determine whether the data had been accessed or modified. Moreover, the FDIC did not ask to examine the employees' non-FDIC computers.

Analysis of the computers could have revealed useful information about the former employees' activities regarding the data, including possible dissemination. The FDIC also could have identified any data remnants from the computer and could have taken appropriate remediation actions.<sup>60</sup>

Absent forensic examination, the FDIC could not be sure whether data had been copied, disseminated, or otherwise shared or compromised.

#### **4. FDIC Statements That the Sensitive Information Was Recovered**

Based on our review of the information provided and interviews conducted for this Special Inquiry, we believe that it is not possible to determine whether all of the sensitive information in these breaches was recovered. The FDIC stated in its notification to Congress for Incidents A, B, D, and E that the device(s) had been recovered from the former employees. Chairman Gruenberg indicated in a response letter to the SST Committee on May 25, 2016, that in each of the six breaches reported to Congress following the Florida Incident, "the information was recovered." While the FDIC may have recovered all but one of the devices, it is not possible to state definitively that the former employees or other individuals did not retain copies of the information.

- Employees-A, B, and D admitted to accessing the drive containing the sensitive information using a non FDIC-issued computer, and our forensic analysis of Employee-C's personal computer indicated that she did as well. The FDIC did not forensically analyze the computers through which the former employees accessed the drives, so the FDIC cannot know whether or not remnants of files containing sensitive information exist on those computers.
- The FDIC did not recover the original device used to download personal and sensitive information in Incident C. As described earlier, in a subsequent forensic analysis of Employee-C's personal computer conducted by the OIG, banking files were discovered that appeared to contain PII.
- In Incident A, the FDIC information was copied onto a new device and the original device used was wiped before being returned to the FDIC. Consequently, once the FDIC recovered the original drive, it did not contain the sensitive information. Employee-E returned a drive that only contained his personal files but did not contain the FDIC files with sensitive information that had been compromised. Employee-D also returned a blank drive with none of the sensitive information he took.

---

<sup>60</sup> Data remnants are data that remain accessible on a computer system or device even after the data have been deleted.

In our interview with then-CIO Gross for this Special Inquiry, he agreed, after being presented with the facts of Incident D, that the information had not been recovered.

### **5. FDIC Statements That the Former FDIC Employees Were Not Computer Proficient**

The issue of an employee's computer proficiency was first raised with regard to the Florida Incident. This breach, and the FDIC's response to it, was the subject of the FDIC OIG's earlier referenced audit entitled *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*. Then-CIO Gross indicated that it was his "inclination" at the time of the breach that Employee-FL was not computer literate and accidentally copied an entire library of files to the portable storage device. We found that Employee-FL submitted a resume when applying to the FDIC in August 2013 that identified classes taken towards a Master of Arts in IT management. The resume was contained in her FDIC personnel file. We also verified that Employee-FL received the degree in March 2013. Further, on February 17, 2016 (prior to the Congressional notification), we informed then-CIO Gross that we had performed an Internet search of Employee-FL's name and identified a public Web page listing various IT courses that she had taken, suggesting that she was familiar with IT concepts and principles.

The FDIC did not reference lack of computer proficiency in any of the notifications it sent to Congress. However, during his Congressional testimony of May 12, 2016, then-CIO Gross stated that the "[i]ndividuals involved in these incidents were not computer proficient."

In addition to the Florida Incident, the facts do not support statements that the former employees were not computer proficient in at least three other incidents where the former employees admitted they downloaded the data on purpose:

- Employee-A's ability to select and download files, wipe the data from the original drive before returning it to the FDIC, and copy data from that drive to the FDIC drive demonstrate his computer proficiency.
- The IRA for Incident D indicated that Employee-D "had a background in IT" and the facts show that it was his practice to execute monthly backups of FDIC data that was relevant to his work.
- Employee-E told OIG investigators that he "consider[ed] himself very technical and often uses external USB devices for his work."

Further, when the OIG interviewed then-CIO Gross, we requested documentation to support his statement that the individuals were not computer proficient. He responded that he had no such documentation.



## **6. FDIC Statements That the Former FDIC Employees Acted Without Malicious Intent**

We did not find information suggesting that Employees-FL, A, B, C, D, E, and F downloaded the sensitive information with the specific intent to cause harm to the FDIC, banks, or any affected individuals.

### **D. Subsequent FDIC Statements Repeated Earlier Assertions and Did Not Correct the Prior Record**

Despite several opportunities to clarify or correct the record, the FDIC did not provide the SST Committee with accurate and complete information about the breaches.

As discussed previously, in the FDIC's notification letters to Congress, the FDIC characterized each breach as "inadvertent." At the Congressional hearing of May 12, 2016, then-CIO Gross repeated this assertion in his written and oral remarks and in response to questions from Members.

Other assertions that were made in the notifications letters to Congress—that the relationship with the former employees (with the exception of Employee-C) "had not been adversarial," and that the FDIC's investigation did not indicate that any sensitive information had been disseminated or the former employees had signed a certification that the data had not been disseminated—were modified slightly in then-CIO Gross' written and oral remarks for the hearing. Then-CIO Gross stated that in each incident "the circumstances surrounding the employee's departure from FDIC employment were non-adversarial" and "there was no evidence that the former employee had disseminated the data."

Then-CIO Gross was aware of facts at the time that would indicate these assertions should not be repeated, or that he should correct the record by correcting the assertion made in the notification letters. IRAs for the seven incidents indicated that then-CIO Gross attended the DBMT meetings where the facts and circumstances of these incidents were discussed. Therefore, then-CIO Gross would have also received the IRAs, which served as the primary source of information regarding each incident. Then-CIO Gross also advised that the basis for not considering these incidents as "major" was largely grounded in his review of the same IRAs. These IRAs, and the DBMT meeting discussions documented therein, contained facts suggesting these assertions were not accurate or complete for all incidents, as discussed in our previous finding.

The FDIC had several opportunities to correct the record regarding these facts and circumstances associated with the breaches but did not do so.

- On May 19, 2016, the SST Committee sent a letter to the FDIC Chairman expressing its concerns that then-CIO Gross' testimony had mischaracterized the breaches and that the FDIC's document production was not complete. The SST Committee stated that there were several instances where then-CIO Gross' responses to questions posed by Members were "false and misleading." The SST Committee requested that the FDIC Chairman review then-CIO Gross' testimony and clarify and/or amend it as necessary and as soon as possible. On May 25, 2016, Chairman Gruenberg responded by stating that the FDIC would review the full, official transcript once received and that additional responses might then be provided. The FDIC did not take this opportunity to promptly address the SST Committee's concerns, even after the transcript became available.
- On May 27, 2016, the SST Committee's Subcommittee on Oversight sent a letter to then-CIO Gross requesting a review of the transcript from the hearing of May 12, 2016, and responses to certain QFRs. On June 20, 2016, then-CIO Gross submitted his transcript corrections and responses to the QFRs. His response did not address any of the substantive issues raised by the Committee during his testimony and in its letter dated May 19, 2016.
- On July 14, 2016, the FDIC had an opportunity to correct the record when Chairman Gruenberg testified before the SST Committee. Chairman Gruenberg reiterated that the FDIC had recovered all the information that had been taken in each of the "major incidents." The only clarification Chairman Gruenberg made was to indicate that while it was not possible to say with certainty that no dissemination had occurred, the FDIC had not identified any dissemination.

In addition, during the May 12, 2016, hearing, then-CIO Gross was asked about the FDIC's selection for a Digital Rights Management ("DRM") tool. He responded that "[w]e have begun the process of identifying the technology . . . What solution set and the timeline for implementing it, we have not identified that as [of] yet." However, then-CIO Gross knew, at the time, that the FDIC was purchasing a 3,000-license pilot of a DRM tool called GigaTrust.<sup>61</sup> Then-CIO Gross explained during his interview with our Special Inquiry team that he did not want to advocate for a particular vendor during the hearing. These statements were not corrected or clarified as part of the responses to SST Committee correspondence.

---

<sup>61</sup> A pilot offers an organization the ability to rollout new technology in small numbers and determine whether it is an appropriate solution.

## **E. The FDIC's Statements Regarding Customer Notifications Overstated Progress**

On several occasions, the FDIC represented that the agency was “in the process” or was notifying individuals that their PII information had been compromised, and offering credit monitoring. For example, in the response to the SST Committee’s QFRs dated May 27, 2016, then-CIO Gross stated that the FDIC was “now in the process of offering credit monitoring services to the individuals at no cost to them to protect any individuals who were potentially affected, and to be responsive to the concerns raised by the members of the Committee.” In addition, during the SST Committee hearing of July 14, 2016, Chairman Gruenberg stated that “[w]e are undertaking notifying and providing credit monitoring to all the individuals affected by those seven breaches.”

At these points in time, on June 20 and July 14, 2016, the FDIC had only decided to notify customers of the data breaches and offer the credit monitoring services. The FDIC had also determined that its existing contract was not adequate to perform these services, and the FDIC established a new contract for credit monitoring and identity theft protection services on June 28, 2016—before the July 14 hearing but approximately 1½ months after deciding to offer the services. Further, the FDIC had just initiated drafting the notification letter to potentially affected individuals—a process that was not completed until as late as November 2016 for some incidents.

In addition, the FDIC did not begin mailing the notifications to potentially affected individuals until November 2016, approximately 4 to 5 months after such statements were made, and with respect to one of the breaches, not until December 2016.

## **F. Recommendations**

We found that the FDIC should have been more timely and precise in its reporting of the breaches. As a result, the reporting might have hindered breach response and recovery efforts. In addition, the reporting and subsequent failure to clarify and correct statements made to Congress may have impeded the ability of Congress to oversee the FDIC’s operations and act to fulfill its duties and address any government-wide impacts.

We recommend that the FDIC:

10. Ensure that its policies, procedures, and practices result in statements and representations to Congress and the American public that are full and complete and reflect the latest information known to agency personnel.

11. Update and correct prior statements and representations made to Congress regarding the incidents addressed in this Special Inquiry where previous information is no longer accurate, valid, or complete.

## **VIII. The FDIC's Document Productions to Congress**

FDIC Circular 1211.2, dated November 9, 2011, described "procedures for handling verbal and written contacts between FDIC staff and Members of Congress and Congressional Staff." According to FDIC Circular 1211.2, OLA was to act as a central contact point for Members and their staff who had inquiries relating to the work of the FDIC. With respect to Congressional correspondence, OLA was to determine which FDIC division or office would be responsible for preparing a draft response to be signed by the Chairman or the Director of OLA. FDIC Circular 1211.2 further stated that "the Chairman places a very high priority on timely and complete responses to Congressional inquiries."

### **A. The SST Committee's Initial Request Regarding Incident F and the FDIC's Response (April 8 and 22, 2016)**

On April 8, 2016, the SST Committee requested that the FDIC produce documents and information related to Incident F, including:

1. All documents and communications referring or relating to [Incident F].
2. A detailed description of the sensitive information copied onto the former FDIC employee's portable storage device.
3. A detailed description of all major security breaches involving FDIC information for the time frame from January 1, 2009 to the present.
4. All documents and communications referring or relating to the FDIC's policies and procedures with respect to safeguarding and handling sensitive information housed on FDIC computer systems.
5. An organizational chart for the Office of the [CIO] and the Office of the [CISO].

The SST Committee letter called for the production of "all responsive documents" within 14 days, by April 22, 2016. The SST Committee letter further requested that "[i]f 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." In addition, the SST Committee letter requested a certification by the FDIC Chairman or his 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.”

On April 11, 2016, OLA Director Jiminez convened a meeting among FDIC personnel to discuss the response to the SST Committee letter dated April 8, 2016. The participants included OLA Director Jiminez and another representative from OLA; then-CIO Gross; five FDIC attorneys from the Legal Division (including three managers); one IT specialist with expertise in responding to document requests; the ISPS Incident Lead; and three representatives from DRR, the FDIC operating division where the former employee, Employee-F, had worked.

Based on our interviews for this Special Inquiry, we learned that OLA Director Jiminez led the meeting and determined what types of documents were going to be produced to the SST Committee. According to the contemporaneous notes of one participant, a Legal Division attorney, OLA Director Jiminez indicated that the FDIC would produce what it believed was necessary for the SST Committee to do its oversight work, and that if the Committee wanted more, it could come back to the FDIC and ask for it. When OLA Director Jiminez heard about the IRA prepared for Incident F, he said that the IRA should be produced in response to the SST Committee’s request.

It was also decided at that meeting that there would be no search of the FDIC’s email vault for responsive documents and communications. We confirmed that no searches of the FDIC’s email vault were, in fact, conducted after the meeting, or before the SST Committee’s hearing on May 12, 2016. In addition, the Legal Division did not initiate a legal hold at that time in response to the request from the Committee on April 8, 2016. Two meeting participants told OIG interviewers that they assumed OLA would discuss the limited production with the SST Committee staff.

In his interview for this Special Inquiry, OLA Director Jiminez stated that his intention with respect to the document production was to provide “as much as we could” within the time given to respond, and to engage in a dialog or discussion with SST Committee staff about how the FDIC could make a production that met the SST Committee’s needs. However, OLA Director Jiminez conceded, and another OLA staff member confirmed, that this approach was not communicated to SST Committee staff at that time or before the Congressional hearing on May 12, 2016.

OLA prepared an initial draft response letter to the SST Committee request of April 8, 2016. An OLA employee, who had just joined the FDIC in March 2016, obtained a sample transmittal letter that OLA had recently used to respond to a different congressional request to use as a template. This sample transmittal letter included language describing the incoming Congressional request for “all documents and communications,” similar to the SST Committee’s request. Moreover, the sample letter indicated that the FDIC’s response was just “an initial partial production” and that the FDIC intended to “continue to review the communications and provide any responsive materials to the Committee on a rolling production schedule as soon as these materials can be made available.”

After undergoing editing within OLA, the FDIC’s response letter to the SST Committee’s request of April 8, 2016, omitted the sample letter’s language acknowledging the nature of the Committee’s request and indications that the FDIC was only making a partial production. Instead, the FDIC’s response letter to the SST Committee simply read:

Your April 8 letter also requested documents and communications referring or relating to the March 18 security incident report. The enclosed DVD provides documents that have been identified as responsive to your request.

The FDIC was aware that it was not producing all relevant documents and communications regarding Incident F. In reviewing OLA’s draft response letter, an FDIC Counsel struck the words, “all communications,” indicating in an email that the response letter should not indicate that this was a complete production—“[w]henver possible, no ‘all.’”

On April 22, 2016, the FDIC provided 118 pages in response to the SST Committee’s request of April 8, 2016, including:

- The IRA for Incident F and letters to and from Employee-F regarding the return of the drive;
- Copies of the notification letters and memoranda to 12 Congressional Committees and government agencies regarding Incident F and the Florida Incident;
- The FDIC’s response to the OIG’s February 19, 2016, Memorandum;
- An FDIC-wide email from Chairman Gruenberg announcing the FDIC’s removable media policy;
- Five FDIC policies bearing on privacy, use of IT, information security, and departing employees; and
- Organizational charts.

The FDIC response letter further noted that the materials contained “personally identifiable information (PII) and sensitive information (SI) about open and operating financial institutions” and that production of such documents did not constitute “a waiver of any privileges that may apply,” including the “deliberative process privilege” or the “attorney-client privilege.” The FDIC further requested that the SST Committee provide “prior notice to the FDIC of any proposed release by the Committee of any non-public information.” In addition, the FDIC stated that “[d]ue to the highly confidential nature of some of the materials being provided, the FDIC requests that at the conclusion of its investigation, the Committee dispose of the materials in a manner that preserves their confidentiality or return the materials to the FDIC.” The FDIC recognized the sensitivity of such information being provided to the SST Committee.

However, the FDIC did not include language in the letter regarding its partial production of documents or possibly a continued effort to search for relevant documents, as it had done in previous response letters to Congress. There was nothing contained in the language of the FDIC’s letter to indicate that there were additional documents or communications that the FDIC intended to produce in response to this request in the future. In addition, the FDIC’s response letter did not include a certification by the FDIC Chairman or his Counsel, as the SST Committee had requested.

### **B. The SST Committee’s Request Regarding the Florida Incident and the FDIC’s Response (April 20 and May 4, 2016)**

On April 20, 2016, the SST Committee sent a letter to the FDIC requesting similar categories of information from the FDIC as the previous letter dated April 8, 2016 – but now relating to the Florida Incident:

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 to or relating to [OMB Memorandum M-16-03].

This SST Committee request dated April 20, 2016 contained the same definitions and instructions as the SST Committee letter dated April 8, 2016, including language that if full compliance could not be made by that date, the FDIC should comply to the extent possible and include an explanation of why full compliance was not possible by that date. In addition, this SST Committee letter requested a certification of the FDIC Chairman or his Counsel.

Again, on April 27, 2016, OLA convened a meeting to discuss the FDIC's response. The decision was made to handle this document request in much the same manner that the FDIC handled the document request of April 8, 2016, regarding Incident F.

On that same day, the FDIC Legal Division initiated a legal hold process to preserve documents related to the SST Committee request. The legal hold was sent to 14 FDIC employees in the Legal Division, DIT, and the Office of Communications. Notably absent from the legal hold issued that day were some key FDIC officials, including: then-CIO Gross, Special Advisor Henning, the then-Acting CISO, prior CISO Farrow, then-DGC McInerney, OLA Director Jiminez, other relevant OLA employees, AGC Griffin, most of the DBMT members, and anyone from the separated employee's operating division. All of these individuals may well have maintained documents that would be responsive to the SST Committee requests. In our OIG interview for this Special Inquiry, the FDIC Counsel who sent out the legal hold did not recall how the 14 employees were identified as recipients of the legal hold and offered no rationale for the selection.

On May 4, 2016, the FDIC responded to the second request from the SST Committee relating to the Florida Incident. This second response letter from the FDIC was similar to the previous response letter dated April 22, 2016—even though the incoming SST Committee letter dated April 20, 2016 requested different types of information than the Committee's letter dated April 8, 2016. The FDIC response letter stated that:

Your April 20 letter requested documents and communications referring or relating to the February 26 security incident report. The enclosed DVD provides documents that have been identified as responsive to your request.

The FDIC produced the following 88 pages of documents, some of which contained redactions:

- The IRA and DBMT minutes for the Florida Incident;
- Emails and correspondence with the departed employee's attorney and the employee's post-employment statements;
- Certain emails between the FDIC and the OIG regarding the Florida Incident;



- The FDIC Legal Division memorandum on the applicability of OMB Memorandum M-16-03 to the FDIC (November 18, 2015); and
- Emails between the FDIC's Office of Communications and the *Federal Times*.

The FDIC response letter similarly noted that the materials contained PII and sensitive information, and that the production did not constitute a waiver of privileges; however, the FDIC failed to include language regarding its partial production or a continued effort to search for relevant documents. Again, the FDIC's response letter did not contain any language to indicate that the FDIC intended to produce additional documents or communications to the SST Committee. At that time, the FDIC had not conducted an email vault search to identify or produce additional responsive documents. In addition, the FDIC's response letter did not include a certification by the FDIC Chairman or his Counsel, as the SST Committee had requested.

On May 6, 2016, at SST Committee staff's request, the FDIC provided an unredacted copy of the May 4 response, and on May 9, 2016, the FDIC provided the SST Committee with two additional documents that were identified as responsive to the request.

### **C. Telephone Call between FDIC Office of Legislative Affairs and SST Committee Staff (May 6, 2016)**

On May 6, 2016, an OLA employee had a telephone conversation with at least two SST Committee staff members. According to SST Committee staff, the Committee had concerns about the completeness of the FDIC's document productions. Accordingly, SST Committee staff said that they asked the OLA employee twice on the call whether the FDIC would certify that all responsive documents had been produced to the Committee. SST Committee staff reported that the OLA employee each time answered in the affirmative.

However, in his OIG interview for this Special Inquiry, the OLA employee said he recalled the question differently: "can you certify that all the documents that you're providing are responsive to the Committee?" The OLA employee believes that he was asked this question once, not twice. The OLA employee said that the documents were responsive.

The OLA employee subsequently advised OLA Director Jiminez about his conversation with SST Committee staff. According to OLA Director Jiminez, the OLA employee said that SST Committee staff "kept asking him if these were all responsive documents, and you know, [the OLA employee] replied yes they were." The OLA employee found SST Committee staff's question to be "odd," and OLA Director Jiminez recalled the OLA employee thought they were "peculiar," but they did not follow up with SST Committee staff.

Both OLA Director Jiminez and the OLA employee stated in their OIG interviews for this Special Inquiry that if asked on May 6, 2016 whether all responsive documents had been produced, the answer would have been, “no.”

On May 10, 2016, Chairman Smith of the SST Committee and Chairman Loudermilk of the SST’s Subcommittee on Oversight sent a letter to the OIG expressing concern that documents had been “apparently withheld by the [FDIC]” and the SST Committee had therefore not received complete document productions from the FDIC. The Chairmen’s letter also stated that the FDIC had certified that it produced all responsive documents, citing the May 6, 2016 telephone call between SST Committee staff and OLA discussed above. The letter further stated that the “FDIC’s decision to withhold responsive materials raises serious questions about the agency’s veracity when communicating with congressional staff regarding the completeness of the agency’s production.” The Chairmen also cited “long-standing concerns about the agency’s willingness to be forthcoming and transparent with Congress” (see Appendix XIII).

Chairmen Smith and Loudermilk, therefore, requested that the OIG provide “any responsive documents that remain outstanding [from the earlier FDIC productions to the SST Committee on April 22 and May 4, 2016].” The OIG provided OLA with a copy of the May 10, 2016, letter that same day. On May 11, 2016, the OIG produced 883 pages to the SST Committee relating to the Florida Incident from our audit work papers and also provided these documents to OLA. The OIG’s production included, among other things, guidance documents, emails, IRAs, DLP reports, CSIRT reports, and DBMT meeting agendas or minutes (see Appendix XIII).<sup>62</sup>

OLA Director Jiminez told OIG interviewers that after reviewing the SST Committee Chairmen’s letter of May 10, 2016, he wanted to send a written response to the SST Committee, and OLA therefore prepared a proposed draft. The draft stated that the “FDIC continues to stand ready to provide the committee with any additional document it believes is responsive to your requests of April 8 and April 20.” According to OLA Director Jiminez, Chairman Gruenberg ultimately directed that a response letter not be sent, as the letter of May 10, 2016, had been addressed to the OIG and not to the FDIC.

---

<sup>62</sup> At the SST Committee’s Subcommittee on Oversight hearing on May 12, 2016, then-CIO Gross stated that, based on his review, the OIG’s 883 page production was “duplicative” of the FDIC’s production and noted that the OIG had produced several versions of the FDIC’s Breach Guide. This was not the case. The OIG produced different iterations and drafts of the FDIC Breach Guide, but not duplicates. We note that, as of date of the hearing (May 12, 2016), the FDIC had not produced any version of its Breach Guide to the SST Committee.

#### **D. SST Committee's Subcommittee on Oversight Hearing (May 12, 2016)**

On April 27, 2016, the SST Committee's Subcommittee on Oversight invited the FDIC Chairman to testify at a Congressional hearing on May 12, 2016, concerning oversight of the FDIC's recent information security breaches. Chairman Gruenberg designated then-CIO Gross to appear in his stead.

At the hearing on May 12, 2016, then-CIO Gross was asked about the FDIC's document productions in response to the SST Committee's two letters. In particular, then-CIO Gross was asked whether the FDIC had produced all documents that were responsive to the SST Committee's requests. Then-CIO Gross stated that the FDIC "made every effort" to be responsive to the Committee's requests and that the FDIC stood ready to provide additional information upon request. Then-CIO Gross further stated that the FDIC's document production was "comprehensive." In addition, he added that the FDIC "made every effort to be quite exhaustive in our response to this Committee."

#### **E. SST Committee Letter to the FDIC Chairman (May 24, 2016) and the FDIC's Subsequent Responses**

On May 24, 2016, Chairman Smith of the SST Committee and Chairman Loudermilk of the SST Committee's Subcommittee on Oversight sent a letter to Chairman Gruenberg expressing concern that then-CIO Gross' testimony of May 12, 2016, was "a misrepresentation, at best, of the strength of the agency's cybersecurity posture." The letter further requested that the FDIC preserve and continue to further identify, gather, and produce responsive documents to the Committee. The Committee's letter also requested that the FDIC make nine named individuals available for a transcribed interview by Committee staff, and included a reminder of the protections for whistleblowers found in the Whistleblower Protection Act.

On June 7, 2016, FDIC General Counsel Yi responded to the SST Committee's letter of May 24, 2016, and provided documents that were responsive to the Committee's request. General Counsel Yi stated that the FDIC was continuing to review documents and would provide responsive materials on a rolling basis. Between May 25, 2016 and June 30, 2016, the FDIC issued a series of legal holds to approximately 246 agency custodians, seven former employees, and 24 third-party vendors. We understand that, as part of this effort, the FDIC continued to provide documents to the SST Committee. Further, SST Committee staff interviewed seven of the nine individuals named in the letter and decided to indefinitely postpone the remaining two interviews.

As noted on page 80, the FDIC had additional interactions with the SST Committee on June 14, June 22, June 28, and August 18, 2016, related to the document production.

## **IX. OIG Findings and Analysis Relating to the FDIC’s Document Production**

### **A. The FDIC’s Initial Productions Were Not Complete and Did Not Comply with SST Committee Instructions**

Prior to the Congressional hearing of May 12, 2016, the FDIC provided a combined 206 pages in response to the SST Committee request letters dated April 8 and 20, 2016. Since that hearing—where several Members stated publicly that the Committee had not received complete productions from the FDIC—the FDIC has produced 75,953 pages of materials responsive to the requests (as of June 2, 2017), including the results of numerous email vault searches. The FDIC has indicated that, after consultation with the SST Committee, it has halted its production efforts, unless the SST Committee makes a request for additional documents.

At the time of the initial document productions, the FDIC did not comply with the instructions—requesting “[a]ll documents and communications”—contained in the SST Committee’s document request letters dated April 8 and 20, 2016. Further, the FDIC did not explain that it had not fully complied, nor provided an explanation. To the contrary, the FDIC removed limiting language from the template used to prepare its response letters.<sup>63</sup> Further, no one from the FDIC had contacted SST Committee staff before the May 12, 2016, hearing to disclose that the FDIC responses were intended to be partial productions. Accordingly, a recipient or reader of the transmittal letters may reasonably infer that the FDIC was attempting to be fully responsive, at the time, to the request and providing relevant materials. This inference is reasonable in light of the SST Committee’s

#### **Excerpts of the SST Committee’s Document Request Letters Dated April 8 and 20, 2016**

“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.”

The SST Committee also requested a certification of the FDIC Chairman or his Counsel 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.”

---

<sup>63</sup> The correspondence for the productions made after the May 12, 2016 hearing made it clear that the productions were partial and ongoing.

instructions about explaining any partial production. The FDIC also did not follow the SST Committee's request that the completeness of the productions be certified in writing.

With respect to the May 6, 2016, telephone call between FDIC OLA and SST Committee staff, SST staff maintains that the OLA employee certified the productions as complete. However, the OLA employee told OIG investigators that he merely said the documents produced were responsive.

Notwithstanding the different recollections of the conversation, the FDIC was aware that the SST Committee staff viewed the discussion as a certification no later than May 10, 2016. On that date, the FDIC received a copy of the SST Committee's letter to the OIG, which stated that the FDIC had "apparently withheld" documents and that the SST Committee had therefore not received complete document productions from the FDIC. The SST Committee's letter also stated that the FDIC had certified that it produced all responsive documents, citing the telephone call between SST Committee staff and the FDIC OLA on May 6, 2016. The FDIC took no action to respond to the SST Committee's understanding.

### **B. The FDIC Did Not Initially Take Sufficient Steps to Identify Responsive Documents**

As referenced earlier in our report, FDIC Circular 5500.5, entitled *Corporate-wide Legal Hold Policy and Implementation*, dated September 5, 2012, placed responsibility with the Legal Division for determining the necessity for and scope of a legal hold and for identifying key players. Specifically, Circular 5500.5 stated that "[d]etermining whether a duty to preserve is triggered [is] based on a good faith analysis and reasonable evaluation of the facts and circumstances as they are known at the time. This analysis may be facilitated by interviews, discussions, and/or meetings with personnel in other divisions who have direct and relevant knowledge of the facts, players, and potentially relevant information." We found no evidence that the Legal Division conducted this analysis in response to the receipt of SST Committee's request for documents on April 8, 2016.

In addition, while the FDIC initiated a legal hold following the SST Committee's request for documents on April 20, 2016, FDIC officials were unable to provide us with a rationale regarding how the FDIC selected which custodians or key players to place on legal hold. A number of individuals that would appear to have direct and relevant knowledge of the facts were not subject to the legal hold—including then-CIO Gross, Special Advisor Henning, the then-Acting CISO and the prior CISO, then-DGC McInerney, OLA Director Jiminez, other relevant OLA employees, AGC Griffin, most of the DBMT members, and representatives from the separated employee's operating division.

Finally, with regard to both requests for documents, the FDIC did not initially conduct searches of the email vault to identify responsive documents. We acknowledge the FDIC did conduct searches of the email vault and issue a broader legal hold following the SST Committee letter of May 24, 2016.

### **C. The FDIC Lacked Specific Policies and Procedures for Responding to Congressional Document Requests**

As discussed in the prior section of our report, OLA Director Jiminez determined, after discussion with representatives from other relevant divisions and offices, what documents were going to be produced to the SST Committee. Based on our work during this Special Inquiry, we identified only one policy that generally addressed responding to Congressional document and information requests—FDIC Circular 1211.2, dated November 9, 2011. This Circular described procedures for handling verbal and written contacts between FDIC staff and Members of Congress and Congressional staff. According to the Circular, OLA was to be a central contact point for Congressional Members and their staff who have inquiries relating to the work of the FDIC and determines which FDIC division or office will be responsible for preparing a draft response to be signed by the FDIC Chairman or the Director of OLA. The Circular did not address who has the authority and responsibility to determine and/or approve the information and/or documents that are provided in response to Congressional document and information requests.

Establishing a single accountable official or “process owner” would help the FDIC ensure appropriate management attention to, and accountability for, responding to Congressional document and information requests.<sup>64</sup> A process owner also would help the FDIC address the “very high priority on timely and complete responses to Congressional inquiries...and assure the consistency of the FDIC’s contacts with Members of Congress and their staff” as stated in FDIC Circular 1211.2. A single accountable official also could clarify accountability for a process that involves multiple divisions and offices.

### **D. Then-CIO Gross’ Statements about the FDIC’s Document Productions Were Not Accurate and the FDIC Did Not Correct the Record**

During the SST Committee hearing on May 12, 2016, then-CIO Gross stated that that the FDIC's document productions were "comprehensive" and "every effort was made for it to be comprehensive." He added that the FDIC "made every effort to be quite exhaustive in

---

<sup>64</sup> The GAO defines a process owner as “an individual held accountable and responsible for the workings and improvement of one of the organization's defined processes and its related subprocesses.” (*Business Process Reengineering Assessment Guide*, May 1997, page 67)

our response to this Committee." These statements were not accurate. At the time then-CIO Gross made them, the FDIC had produced only 206 pages of responsive documents. The FDIC has now produced 75,953 pages of responsive documents.

Then-CIO Gross had previously participated by telephone in the OLA meeting of April 11, 2016, where it was decided to provide the SST Committee only limited documents relating to Incident F. In addition, the FDIC decided at this meeting that there would be no search of the FDIC's email vault.

According to our OIG interviews for this Special Inquiry, OLA Director Jiminez and Special Advisor Henning stated that then-CIO Gross was specifically advised, in preparatory meetings prior to his testimony on May 12, 2016, that he should not say that the FDIC had produced all documents to the SST Committee. OLA Director Jiminez stated that then-CIO Gross was advised to say that the FDIC had tried to be "responsive" to the SST Committee's requests. Special Advisor Henning also identified "talking points" that were prepared for then-CIO Gross' testimony, which included:

- We believe that the documents we provided are directly responsive to the Committee's April 8 and April 20 requests.
- We made no representation that the production was exhaustive, it was a bona fide effort to provide the Committee with information regarding the incidents that were previously reported.

When asked in his interview for this Special Inquiry whether he was cautioned during his hearing preparation not to state that all responsive documents had been produced, then-CIO Gross responded "I don't recall that." Neither then-DGC McInerney nor the OLA employee could recall whether the completeness of the FDIC's document production was discussed during then-CIO Gross's hearing preparation.

When interviewed by the OIG, then-CIO Gross maintained that at the time of the hearing on May 12, 2016, he assumed that OLA had been fully responsive to the SST Committee's requests and that the first time he learned of the SST Committee's concerns about the FDIC's document productions was at the hearing itself. Then-CIO Gross said in his OIG interview for this Special Inquiry that he could not recall whether or not he was aware of the SST Committee's letter dated May 10, 2016, prior to the hearing.

As discussed below, FDIC personnel agreed that then-CIO Gross' characterizations of the FDIC productions as "comprehensive" or "exhaustive" were inaccurate. Even then-CIO Gross told us that, based on what he knew at the time he was interviewed, he realized that the productions were not complete.

In his interview, OLA Director Jiminez stated that his intention with respect to the production was to provide “as much as we could” within the time given to respond. When asked if the FDIC’s efforts were exhaustive, he said: “Exhaustive? I would not say that we performed an exhaustive search.” The OLA employee also agreed that the FDIC efforts were not exhaustive.

In reviewing OLA’s draft response letter for the first production, a Legal Division attorney struck the words, “all communications,” indicating in an email that “[w]henver possible, no ‘all.’” In her interview, the Legal Division attorney characterized the production as “initial preliminary” and that “[a]n initial production can’t be by its very nature comprehensive. It’s an initial production.”

During Chairman Gruenberg’s interview for this Special Inquiry, he stated that it was “fair to say, the use of the word ‘comprehensive’ was not the best choice of words. I don’t take issue with that.”

## **E. Recommendations**

Congressional Committees use document requests to gather information about how programs are being implemented, statutes are being followed, and funds are spent, among other things. Agencies are expected to cooperate and work in good faith to identify and produce the records that are responsive to Committee requests. As it relates to our Special Inquiry, the SST Committee was examining the FDIC’s handling of “major incidents,” its data security policies, and reporting of data breaches as “major incidents.” In connection with its examination, the Committee requested that the FDIC produce relevant documents and information.

As described in this section of our report, our Special Inquiry found that the FDIC should have responded to the initial requests in a more complete manner. The FDIC also should have been clear in its communications with and testimony before the SST Committee regarding its approach and progress in complying with document production requests. Accordingly, we recommend that the FDIC:

12. Clarify legal hold policies and processes to ensure that all relevant personnel and sources of documents and information are included in the scope of legal holds.
13. Ensure that Congressional communications policies, procedures, and guidelines establish a single office that has accountability and authority for providing



timely responses compliant with Congressional requests and communicating with Congressional staff regarding those requests.

## **X. Conclusion**

Our work revealed certain systemic weaknesses that hindered the FDIC's ability to handle multiple information security incidents and breaches efficiently and effectively; contributed to untimely, inaccurate, and imprecise reporting of information to Congress; and led to document productions that did not fully comply with Congressional document requests in a timely manner. In addition, our work found shortcomings in the performance of certain individuals in key leadership positions.

The FDIC had not taken sufficient steps at the time of the New York and Florida Incidents (September and October 2015) to ensure that it had a comprehensive incident response program and plan that addressed current statutory requirements, most notably those associated with "major incidents." In this regard, we found that the approach adopted by then-DGC McInerney and her apparent reluctance to create electronic records delayed the Legal Division's provision of legal guidance on whether and how FISMA 2014 and OMB implementing guidance on reporting incidents applied to the FDIC. In turn, this contributed to a delay in the FDIC's incident response and postponed the reporting of the "major incidents."

The FDIC also did not consistently adhere to existing policies in its Data Breach Handling Guide, especially with respect to carrying out and documenting risk assessments and the underlying analysis for key decisions. These policies called for the FDIC's DBMT to serve as a key component of the FDIC's incident response, including to examine the facts and circumstances surrounding an incident, and submit a recommendation to the CIO regarding an appropriate course of action. The CIO led the DBMT and was responsible for reviewing and determining whether to accept the DBMT's recommendation, including breach notifications to individual consumers whose PII had been compromised and provision of credit monitoring services. The CIO also was required to notify the Executive Office (including the FDIC Chairman) of the recommended course of action regarding data breach notification to consumers and other external communications.

Then-CIO Gross did not fulfill his responsibilities for ensuring these activities were properly implemented. For example, then-CIO Gross made a recommendation to senior FDIC leadership regarding the reporting of the Florida Incident without input from the DBMT and its deliberations. Further, he failed to document in written form a rationale for his recommendation to the FDIC Chairman. Consequently, the FDIC lacked complete

information for determining a proper course of action. Further, then-CIO Gross' actions related to the Florida Incident appeared to influence the DBMT's reviews of other incidents, namely determining risk levels without fully considering and/or documenting the unique circumstances and risks involved.

The FDIC did not fully consider the range of impacts on bank customers whose information had been compromised or consider customer notification as a separate decision from whether it would provide credit monitoring services. In addition, given the number of individuals potentially affected by the breaches, the FDIC did not dedicate sufficient personnel and contractors to handle customer notification activities in a timely manner. As a result, the FDIC delayed notifying consumers and thus precluded them from taking proactive steps to protect themselves.

As the Senior Agency Official for Privacy, then-CPO Gross should have carried out his responsibilities related to breach response, particularly those associated with reducing the risk of harm to potentially affected individuals. He also should have documented, in written form, his recommendations to the Chairman regarding customer notification of data breaches and offerings of credit monitoring services, and an explanation of his rationale for such recommendations. Absent that documentation, the FDIC was not able to establish measurable benchmarks to ensure consistency in its decision-making, such as whether potentially affected individuals would be notified and the timing of the notifications.

When faced with assessing the risks associated with the incidents and recovering the data involved, the FDIC unduly relied on post-employment statements of former employees. These statements lacked weight and credibility, and were similar to the Pre-Exit Clearance Forms and data questionnaires on which the employees denied taking data. Also, portions of the statements—prepared by the FDIC—were contradicted by the facts known at the time. Further, the Pre-Exit Clearance Forms and data questionnaires themselves lacked adequate acknowledgments and warnings to employees regarding breaches of sensitive information. The FDIC was not able to hold former employees accountable for their actions.

We determined that, based on the information known to the DBMT, the FDIC's reporting of the "major incidents" to Congress should have been more timely and precise. The FDIC used broad characterizations and referenced mitigating factors that were sometimes inaccurate and imprecise, and tended to diminish the potential risks. Throughout the incident response risk analysis and mitigation process, the CIO received and was responsible for evaluating information from the DBMT on incident risk, impact, and

mitigation. The CIO was also responsible for keeping FDIC officials informed of the status of an ongoing incident response. As a result, then-CIO Gross should have known that certain statements to Congress were not consistent with the facts known to the FDIC at the time. He should have been more precise in statements regarding individual incidents, since each incident had its own set of facts and circumstances, and he should have provided updated information to Congress as new information was discovered.

In addition, despite several opportunities, the FDIC subsequently did not correct earlier statements made to Congress regarding the nature of the incidents. The FDIC also could have provided more comprehensive responses to Congressional document requests. OLA, under the direction of Director Jiminez, should have maintained a clear and timely record of communications with Congressional staff, and should have corrected the record once the FDIC became aware that it had made an inaccurate statement or obtained updated information. With respect to document requests, Director Jiminez and his staff should have thoroughly discussed the initial document requests with SST Committee staff, including how the FDIC could accommodate the requirements, and ensured that the SST Committee was aware that the FDIC was not immediately producing all responsive documents.

Further, when the SST Committee requested documents in April and May 2016, the FDIC's initial document productions were not complete and did not comply with SST Committee instructions. The Legal Division was involved in how the documents would be collected by the FDIC. In that regard, certain attorneys in the Legal Division did not have a clear rationale for not initially implementing a legal hold, nor for the selection of custodians or key players upon which legal holds were eventually issued. As a result, the FDIC did not search for responsive documents from all relevant FDIC sources until after May 24, 2016, when the SST Committee requested that the FDIC specifically preserve all pertinent documents concerning the FDIC's cyber security posture and information related to data breaches.

Throughout and subsequent to our Special Inquiry, the FDIC took steps to address prior recommendations pertaining to incident and breach response. In addition, we made 13 recommendations in this Special Inquiry report to address the systemic issues associated with the FDIC's incident response and reporting and interactions with Congress. With respect to the shortcomings in performance that we identified, the FDIC should review the facts and analysis that we have developed in this Special Inquiry report and advise the FDIC OIG of any actions undertaken to address them.

## **XI. Comments from the FDIC and Former FDIC Officials**

We provided an initial draft of this report to the FDIC and requested feedback on factual accuracy. We subsequently issued a draft for formal comment on March 12, 2018. The FDIC Chairman provided a written response dated March 26, 2018. The response is presented in its entirety in Appendix XVII.

The FDIC concurred with the report's 13 recommendations. The FDIC has completed responsive corrective actions for two of the recommendations and we consider them closed. The FDIC has proposed actions to address the remaining 11 recommendations and plans to implement them between June 2018 and December 2018. These recommendations will remain open until the OIG determines that planned actions have been completed and are responsive to the recommendations. Appendix XVIII contains a summary of the FDIC's corrective actions.

We also shared a draft with former CIO Gross and former DGC McInerney through their respective Counsel, and both provided written responses. The response prepared on behalf of former CIO Gross stated that his performance should be viewed in the context of his having been appointed to the position in November 2015; he was not involved in scoping, searching, or compiling documents responsive to the SST Committee's document request of April 8, 2016; and he was not advised to testify that the FDIC had not produced all of the Committee's requested documents.

We considered these points and reviewed our Special Inquiry interviews and supporting documentation to ensure that our report was factually correct. We clarified certain items relating to his testimony preparation with respect to the document production. Otherwise, our evidence did not support further revisions.

The response prepared on behalf of former DGC McInerney expressed concerns regarding the report's references to FISMA 2014 and OMB Memorandum M-16-03 reporting requirements as they related to the New York Incident; her interactions with AGC Griffin regarding the Legal Division guidance on the definition of a "major incident" and FISMA 2014 reporting requirements; and her approach to developing legal guidance and delays in the reporting of incidents to Congress.

We similarly reviewed our evidence and made clarifying revisions to the report as we deemed appropriate. The revisions did not change our conclusions.

## Objective, Scope, and Methodology

---

### Objective

The objective of this Special Inquiry was to review the facts surrounding the incidents and the FDIC's original decision not to report the "major incidents" to Congress, and examine representations made by the FDIC and its initial responsiveness to requests from the SST Committee for documents. This Special Inquiry also addressed the extent to which the FDIC had developed and implemented certain policies and procedures relevant to the handling and reporting of the incidents.

This Special Inquiry was conducted in accordance with OIG policy and procedures by an interdisciplinary team including attorneys, investigators, forensic accountants, and a program analyst. Each member of the team was required to conduct the special inquiry with due professional care in the performance of their work, in a fair and balanced manner, and in conformance with the generally accepted standards of conduct for government employees. We believe the evidence obtained provides a reasonable basis for our findings and conclusions.

### Scope and Methodology

To address the Special Inquiry objective, we reviewed and considered statutes, authorities, standards, guidance, policies, programs, and procedures relevant to data protection and incident response. Specifically, we identified and reviewed:

#### Statutes

- The Federal Information Security Management Act of 2002
- The Federal Information Security Modernization Act of 2014
- The Paperwork Reduction Act of 1995
- The E-Government Act of 2002
- Section 522 of the Consolidated Appropriations Act of 2005

#### Executive Order

- Executive Order 13719, Establishment of the Federal Privacy Council

#### OMB Policy and Guidance

- Circular A-130, Management of Federal Information Resources, November 28, 2000
- Circular A-130, Managing Information as a Strategic Resource, July 28, 2016

## Objective, Scope, and Methodology

---

- Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy
- Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements
- Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information
- Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

### NIST Guidance

- SP 800-61, Revision 2, Computer Security Incident Handling Guide

### FDIC Legal Opinions, Policies, Procedures, and Guidance

- Legal Division Opinion, Applicability of OMB Memorandum M-16-03, dated November 18, 2015
- Circular 1360.9, Protecting Sensitive Information, dated April 30, 2007
- Data Breach Handling Guide, Version 1.4, dated April 16, 2015, and Version 1.5, dated June 6, 2016
- Circular 2150.1, Pre-Exit Clearance Procedures for FDIC Employees, dated September 3, 2014
- Circular 1211.2, Congressional Contacts and Correspondence, dated November 9, 2011
- Circular 5500.5, Corporate-wide Legal Hold Policy and Implementation, dated September 5, 2012

We evaluated the FDIC's activities for the breaches examined in the Special Inquiry against the statutes, authorities, standards, guidance, policies, programs, and procedures that were in effect at the time the FDIC discovered and addressed those breaches. We considered new guidance issued by OMB and relevant updates to the FDIC's policies, procedures, and guidelines when developing our findings, conclusions, and recommendations. We specifically performed the following work:

- evaluated FDIC guidance for implementing statutes and guidance governing breach response;

## Objective, Scope, and Methodology

---

- obtained and reviewed IRAs and other documentation related to DBMT activities for the breaches addressed by the Special Inquiry;
- prepared timelines of key breach response activities associated with all breaches reviewed;
- reviewed pre-exit clearance forms, data questionnaires, and statements of former employees who improperly took the FDIC's sensitive data;
- evaluated whether the FDIC met statutory incident reporting requirements, including notifying potentially affected individuals;
- reviewed the FDIC's "major incident" notifications to Congress and other appropriate government agencies;
- reviewed statements in testimony and correspondence between the FDIC and Congress related to the breaches we reviewed; and
- obtained documentation and interviewed officials associated with the FDIC's production of documents and information requested by Congress.

In carrying out this work, the Special Inquiry team:

- gathered documents from witnesses and retrieved email based on various search parameters from the FDIC vault, including whole stores of certain employees' emails for designated periods of time and topical search terms designed to retrieve relevant documents;
- conducted a judgmental review of thousands of emails and other documents within that population;
- reviewed 75,953 pages of documents ultimately produced by the FDIC to the SST Committee; and
- interviewed 24 current or former FDIC employees, and six former employees who committed breaches that were the subject of this Special Inquiry.

In addition, the Special Inquiry team reviewed joint interviews of former employees performed by OIG and FinCEN special agents to understand additional information about the former employees, why they downloaded the data, and how they handled the data.

## The Senate Banking Committee's June 28, 2016 Letter to the OIG and the OIG's July 29, 2016 Response



June 28, 2016

Mr. Fred W. Gibson  
Acting Inspector General  
Federal Deposit Insurance Corporation  
Office of Inspector General  
3501 Fairfax Avenue  
Arlington, VA 22226

Dear Mr. Gibson,

A series of data breaches at the Federal Deposit Insurance Corporation (FDIC) has compromised sensitive financial information in the FDIC's possession, including suspicious activity reports, the resolution plans for some of the largest U.S. banks, and bank customers' social security numbers.

According to a memorandum dated February 19, 2016, your office reviewed the response to one such incident in Gainesville, Florida, and concluded that senior FDIC officials failed to properly classify that incident as "major," did not adequately document their decision-making process, applied factors not authorized by Office of Management and Budget guidance, and failed to timely report the breach to Congress.

The FDIC has since retroactively reported at least six more major incidents, in addition to reports of a criminal investigation of a former employee who removed information related to banks' resolution plans in 2015, and an ongoing investigation into a leak of the most recent living wills results. Furthermore, a former employee is being prosecuted in federal court in Illinois over confidential information taken from the agency in 2012, and recent media reports have revealed to the public for the first time a highly sophisticated attack beginning in 2010 that infected the computers of many top FDIC executives, including former Chairman Sheila Bair.

The Federal Information Security Modernization Act of 2014 requires agencies to promptly report major data breaches to Congress. I understand that your office is currently conducting an audit of the FDIC's controls for major data security incidents. While audits are critical to identifying deficiencies and improving agency performance, the possibility that FDIC officials repeatedly failed to fulfill FDIC's statutory obligations merits additional scrutiny. I request that the scope and depth of your on-going review of each major data security incident be no less thorough than the work undertaken by your office in connection with the Gainesville incident. I further request that your on-going review examine any broader institutional problems at the FDIC related to data security, breach reporting, and policies governing departing



**The Senate Banking Committee's June 28, 2016 Letter to the OIG and the  
OIG's July 29, 2016 Response**

---

employees' access to sensitive financial information. Moreover, I request that you consider whether any representations made by FDIC officials are inconsistent with the findings of your review, and whether such representations were fully forthright and complete.

Thank you for attention to this matter.

Sincerely,

A rectangular box with a black border, used to redact the signature of Richard Shelby.

Richard Shelby  
Chairman

## The Senate Banking Committee's June 28, 2016 Letter to the OIG and the OIG's July 29, 2016 Response



**Federal Deposit Insurance Corporation**

3501 Fairfax Drive, Arlington, Virginia 22226

Office of Inspector General

TRANSMITTED VIA ELECTRONIC MAIL

July 29, 2016

Honorable Richard Shelby  
Chairman  
Committee on Banking, Housing, and Urban Affairs  
U.S. Senate  
Washington, D.C. 20510-6075

Dear Chairman Shelby:

We have had the opportunity to carefully review the request that the Senate Banking Committee submitted to our office on June 28, 2016. I am writing to advise you of work we have completed, as well as currently underway or planned, to address the concerns you raise.

On July 8, 2016, our office publicly released two audit reports, entitled *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* and *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans*. Those reports address the first major information security incident reported by the FDIC, hereinafter referred to as the "Florida Incident," and a second incident involving an FDIC employee who abruptly resigned and took sensitive resolution plan information without authorization. These two audits are relevant to the concerns raised in your letter.

Additionally, we have opened a Special Inquiry that will explore the facts surrounding the other six major information security incidents that the FDIC has reported to the Congress. We will compare those facts with representations made to the Congress by the FDIC about those incidents. Because the Committee's request also asks us to consider the FDIC's forthrightness more broadly, the Special Inquiry will also address the FDIC's initial responsiveness to a request from the Committee on Science, Space, and Technology of the House of Representatives for documents related to the Florida Incident, other major incidents, the FDIC's data security policies, and the FDIC's original decision not to report major incidents to the Congress.

Moreover, we are currently conducting two additional audits that bear on the issues raised in your letter. First, we are auditing the effectiveness of the FDIC's information security program and practices as required by the Federal Information Security Modernization Act of 2014. This audit, which will be completed in November 2016, will provide a broad perspective on the FDIC's cybersecurity posture. We are also conducting an audit of the FDIC's efforts to address prior recommendations made by our office pertaining to employee and contractor credentialing and multifactor authentication. We expect to complete this audit in October 2016.

## The Senate Banking Committee's June 28, 2016 Letter to the OIG and the OIG's July 29, 2016 Response

We also plan to initiate several new assignments in areas pertinent to the Committee's ongoing oversight of the FDIC throughout the fall of 2016:

1. The FDIC's controls for evaluating the risk of harm to individuals potentially affected by breaches involving personally identifiable information and the FDIC's procedures for notifying and providing services to affected individuals.
2. The FDIC's ability to prevent and detect network intrusions.
3. The FDIC's pre-exit clearance procedures designed to mitigate the risk of employees and contractors taking sensitive information from the FDIC upon departure.
4. The FDIC's use of its enterprise architecture and strategic information technology (IT) planning techniques to ensure a secure, reliable, and modern IT environment.
5. The FDIC's controls over its network interconnections with outside organizations.

We will keep the Committee advised of our timetables for completing the assignments described above as we finalize our work plans.

Finally, our office issued a report on May 24, 2013, entitled *Investigation of Division of Information Technology (DIT) Computer Security Incident*, detailing the results of our investigation of DIT's handling of a serious computer security incident involving the penetration of the FDIC's network by an advanced persistent threat (APT). At the time, we notified this Committee, and others, of our investigation of the FDIC's handling and reporting of the matter, and offered briefings. Shortly after our report was provided to the FDIC, the FDIC's Chief Information Security Officer (CISO) announced his retirement and the FDIC restructured the roles and responsibilities of the Chief Information Officer (CIO), CISO, and Information Security and Privacy Staff. One outcome of this restructuring was that the roles and responsibilities of the CIO and DIT Director were separated. Both positions had previously been held by the same individual.

Additionally, we are looking into whether instructions may have been given to FDIC employees to obscure and/or delay remediating the APT because of the timing of the FDIC Chairman's confirmation process. We have opened a Special Inquiry to review these serious allegations.

If you have any questions, please feel free to contact me at [redacted] or [redacted]. [redacted] of my staff is also available to assist you and can be reached at [redacted] or [redacted].

Sincerely,

[redacted signature]  
Fred W. Gibson, Jr.  
Acting Inspector General

cc: Honorable Sherrod Brown, Ranking Member  
Committee on Science, Space, and Technology of the U.S. House of Representatives  
Committee on Financial Services of the U.S. House of Representatives

Pre-Exit Clearance Record for Employees

Federal Deposit Insurance Corporation  
**PRE-EXIT CLEARANCE RECORD FOR EMPLOYEES**

**INSTRUCTIONS:** This form must be completed and submitted at least one week prior to the last day of duty status. It is the responsibility of the employee to take the necessary steps to ensure that proper clearance is secured. The employee will obtain clearance from each appropriate office listed below. The Administrative Officer or his/her designee will assist the separating employee in the clearance process. Failure to complete this form may delay the employee's final salary and/or lump sum annual leave check.

**NOTE:** Employees must list all index relevant business documentation on form FDIC 2150/03, Data Questionnaire for Departing/Transferring Employees/Contractors, Section VI, Data Collection Index.

1. Employee's Name <i>(Please type or print)</i>	2. FDIC Employee ID	3. Position Title	4. Grade
5. Current Duty Station <i>(City, State, Division, Office)</i>		6. Home Telephone No.	7. Work Telephone No.
8. Forwarding Address <i>(Street, City, State, and ZIP Code)</i>		9. Mailing Address <i>(if different from No. 8)</i>	

10. Type of Action *(Check applicable box)*

Reassignment within FDIC to *(Specify)* \_\_\_\_\_  Separation *(Specify)* \_\_\_\_\_

Transfer to another Federal agency *(Specify)* \_\_\_\_\_

11. Division/Office	Clearance			12. Date	13. Signature/Remarks
	YES	NO	NA		
<b>A. ADMINISTRATIVE OFFICER OR DESIGNEE</b>					
Outstanding Training Request					
Blanket Travel Orders					
Credit Card <i>(Travel)</i>					
Credit Card <i>(Purchase)</i> - RECEIVED					
Convenience Checks <i>(Procurement)</i> - RECEIVED					
Notify FDIC Purchase Card Agency Program Coordinator					
Purchase Card File - RECEIVED <i>(with outstanding receipts and invoices)</i>					
Exit Survey link provided					
Exit Interview Notification provided to employee					
Other <i>(List)</i> _____					
<b>B. IMMEDIATE SUPERVISOR</b>					
Publications/Manuals					
Office Equipment					
In-House Electronic and Paper Records					
<i>(List all relevant business documentation on form FDIC 2150/03, Records and Information Management Questionnaire for Departing/Transferring Employees)</i>					
Sensitive PII secured or disposed of					
<b>C. TIMEKEEPER</b>					
Leave Balance ST _____ AL _____ Other _____					
Other <i>(List)</i> _____					
<b>D. DEPUTY ETHICS COUNSELOR/EXECUTIVE SECRETARY SECTION</b>					
Post Employment Briefing					
Termination Reporting Packet <i>(“EM” level employees only)</i>					
Other <i>(List)</i> _____					
<b>E. DIVISION OF INFORMATION TECHNOLOGY</b>					
Laptop Computers, PDA's, etc.					
Telephone Calling Card(s) <i>(FTS, GETS)</i>					
SafeWord Token					
Access Control					
Other <i>(List)</i> _____					
<b>F. DIVISION OF FINANCE</b>					
Credit Card <i>(Travel)</i> verify receipt with AO					
Travel Audit					
Travel Policy - Relocation					
Receipts, Receivables & Vendor Maintenance Unit					
Other <i>(List)</i> _____					

FDIC 2150/01 (6-14)

Pre-Exit Clearance Record for Employees

11. Office/Division (Cont'd)	Clearance			12. Date (Cont'd)	13. Signature/Remarks (Cont'd)
	Yes	No	NA		
	If no, explain under remarks				
<b>G. DIVISION OF ADMINISTRATION (DOA)/ HUMAN RESOURCES BRANCH</b>					
Employee Benefits					
Payroll/Personnel					
Release for Salary					
Other (List) _____					
<b>H. DOA/CORPORATE SUPPORT SECTION, CSB</b>					
Library Material/On-line Database Passwords					
Office of Workers Compensation Program Coordinator					
Corporation/Official Records					
Other (List) _____					
<b>I. DOA/SECURITY &amp; EMERGENCY PREPAREDNESS SECTION, CSB, OR FIELD FACILITIES MANAGER</b>					
Parking Permits					
Transit Subsidy					
ID Badges					
Access Cards					
Building/Office Keys					
Other (List) _____					
<b>14. Administrative Officer/Designee Certification</b>					
I certify that all required levels of clearance have been/have not been obtained for the below-named employee.					
Administrative Officer's Signature				Date	
<b>15. Employee's Certification</b>					
I certify that:					
All Corporation-owned property, equipment, and documents that were in my possession have been returned to the proper division/office or have been accounted for. I certify that all debts owed by me to the Corporation have been settled. I further certify that I have removed all software loaned to me by the Corporation from my personal computer.					
(i) I have not removed any Confidential Information (as defined below) from FDIC premises except as necessary or appropriate in the course of my employment, disclosed any Confidential Information to any person not authorized to receive it, nor sent any Confidential Information to any address outside the FDIC (whether by mail, email or otherwise) except in accordance with applicable FDIC policies on the use and transmittal of FDIC information, and (ii) I have returned to the FDIC all Confidential Information that I possessed (in whatever form it existed) and will not transmit or remove (in any format or in any medium) any Confidential Information to any address outside the FDIC between the signing of this certification and my departure from FDIC employment.					
As used above, "Confidential Information" means information that I came to possess by virtue of my employment with the FDIC that is or was confidential either (i) of a personal nature (sometimes referred to as "Personally Identifiable Information" or "PII") or (ii) as it relates to certain commercial interests, to banking or financial institutions or the banking or financial industry in general, or to the overall programs and mission of the FDIC (sometimes referred to as "Sensitive Information").					
I further acknowledge that I am obligated to maintain the confidentiality of Confidential Information extending beyond the termination of my employment by the FDIC.					
If there is a breach of this agreement, the FDIC shall be entitled to injunctive relief from such court or courts as shall have jurisdiction and such relief shall be in addition to, and not in lieu of, other remedies available to the FDIC under the law. I further acknowledge that the FDIC shall be entitled to recover reasonable costs and attorney's fees in connection with obtaining any such injunctive relief.					
My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (see 18 U.S.C. 1001).					
Employee's Signature				Date	
REMARKS:					
<b>PRIVACY ACT STATEMENT</b>					
Collection of this information is authorized by 12 U.S.C. § 1919 and Executive Order 9397, as amended. The requested information will be used by FDIC personnel for clearing employees leaving the Corporation, to certify the return of FDIC property previously issued to the departing employee, and to ensure that all outstanding financial indebtedness to the FDIC has been settled. Disclosures of information on this form may be made to appropriate Federal or state agencies for enforcement if a violation or possible violation of civil or criminal law is discovered; the U.S. Office of Personnel Management, and other appropriate agencies or offices to the extent disclosure is necessary to carry out government-wide personnel management, investigatory, and adjudicatory functions; to the General Accounting Office for inspection by auditors; and, to a Congressional office in response to an inquiry made at the request of the individual. This information may also be disclosed in accordance with the other "routine uses of records" listed in the U.S. OPM's Official Personnel Files System, OPM Gov-1. Your Social Security Number (SSN) is requested to ensure record accuracy. Completion of this form is voluntary, but failure to provide the requested information, including your SSN, may result in the delay of releasing your final salary and/or lump sum check(s).					
FDIC 2150/01 (6-14) Page 2					

Data Questionnaire for Departing/Transferring Employees/Contractors

Federal Deposit Insurance Corporation

**DATA QUESTIONNAIRE FOR DEPARTING/TRANSFERRING EMPLOYEES/CONTRACTORS**

1. Check applicable box for person completing the form:  
 Executive     Designee     Self

**INSTRUCTIONS:** At least 1 week, but no more than 30 days, prior to employee's/contractor's departure/transfer, the supervisor/oversight manager shall inquire about relevant data in the possession or control of the employee/contractor.

**SECTION I – DEPARTING/TRANSFERRING EMPLOYEE/CONTRACTOR INFORMATION**

2. Employee/Contractor Name	3. Date	4. Division/Office	5. Location	6. Region
8. Requested Action (Check applicable box) <input type="checkbox"/> Departing <input type="checkbox"/> Transferring	9. Departure Date	10. Transfer Date	11. Supervisor/Oversight Manager	12. Records Liaison <input type="checkbox"/> Contractor <input type="checkbox"/> Intern

**SECTION II – LEGAL HOLD INFORMATION**

13. To your knowledge or recollection, are you subject to an existing Legal Hold?     YES     NO

13a. If YES, above, what case or legal matter? \_\_\_\_\_

13b. Who is the Oversight Attorney? \_\_\_\_\_

**NOTE: FOR QUESTION 11 ABOVE, if departing employee/contractor appears to be subject to a LEGAL HOLD, contact the Oversight Attorney for the matter and determine whether departing employee/contractor are still subject to HOLD and, if so, what documents should be retained.**

**SECTION III – DATA LOCATION ON-SITE**

14. Where do you save your documents and how are they organized (Check ALL that apply and provide an explanation)

14a.  Hard Drive \_\_\_\_\_

14b.  Network personal folders \_\_\_\_\_

14c.  Network shared folders \_\_\_\_\_

14d.  SharePoint \_\_\_\_\_

15. Do you maintain hardcopy files?     YES (If yes, provide locations in 15a.)     NO

15a. Where are the locations of your hardcopy files?  
 16. Which shared drive(s), SharePoint, shared mailboxes, etc., do you use?

**NOTE: If relevant information exists in these repositories, document in Section VI, Data Collection Index.**

17. Do other employees place or maintain documents you create or edit on a shared drive for you in electronic format?  
 YES (If yes, provide response in 17a.)     NO

17a. Provide Names of Employee(s)

**NOTE: FOR QUESTION 15 ABOVE, duplicate items HELD by these employees should be deleted/destroyed unless subject to LEGAL HOLD.**

**SECTION IV – DATA LOCATION OFF-SITE**

18. Are there other locations where FDIC documents might be held?  
 YES (If yes, provide locations in 18a.)     NO

18a. Other locations (Check ALL that apply)  
 Home Computer     Personal email accounts     Portable electronic files, such as DVDs, CDs, Thumb Drives

FDIC 215003 (10-14)

Data Questionnaire for Departing/Transferring Employees/Contractors

**SECTION IV – DATA LOCATION OFF-SITE (CONT'D)**  
 18b. If "YES" to any in Item 18a, list types and locations

**NOTE: FOR QUESTION 16 PREVIOUS PAGE.** Ensure that FDIC documents on non-FDIC equipment of departing employee/contractor are moved to FDIC equipment and preserved following appropriate procedures once moved, the items should be deleted from non-FDIC equipment.

**SECTION V – DATA POINT OF CONTACT**  
 19. Are you the data point of contact  YES (If YES, check ALL that apply and list in 19a.)  NO  
 Shared Mailbox  Shared Folder  SharePoint Site  
 19 a List Shared Mailbox, Folder, and/or Site Information

**NOTE: FOR QUESTION 17 ABOVE.** Determine whether it is necessary to maintain the shared mailbox folder or site depending on the answer, initiate action to delete the site or establish a new point of contact and ensure proper access is assigned.

**SECTION VI – DATA COLLECTION INDEX**

20. List all relevant business documents to include record files or folder names, application/repository, and records and data locations or file path. See below shaded example on how to capture data index information.

EX	Record/File or Folder Name	Application/Repository	Storage Format	Records/Data Location or File Path	Does a Co-worker have access?		IT Owner? DOA	PII? No	If Encrypted, Provide Password to Supervisor	Records Description/Comments
					YES	NO				
1	Transit subsidy	Adobe Professional XP	Electronic	S:\DOARECORDS\RIMU\FORMS					ZZ73JU	Shared RIMU Folder
2										
3										
4										
5										
6										
7										

**SECTION VII – COMMENTS**  
 21. Given the history with the various kinds of records and matters that you have had responsibility for, do you have recommendations for appropriate handling of any of the categories of materials that we have discussed?

**SECTION VIII – APPROVAL AND SUBMISSION (Records Liaison shall submit completed form to the Records Management Assistance Center Mailbox)**  
 22. Records Liaison \_\_\_\_\_ Date \_\_\_\_\_

**Former Employees' Statements**  
**Employee-FL**

---

**DECLARATION OF** [redacted]

1. My name is [redacted] I am over 18 years of age.

2. I was employed by the Federal Deposit Insurance Corporation (FDIC) from [redacted] until I resigned effective October 16, 2015.

3. On December 8, 2015, in response to a December 2, 2015 letter from the FDIC, [redacted] delivered to FDIC staff a Western Digital "My Passport Elite" 500 GB, USB 2.0 portable external drive, serial number [redacted] ("Western Digital Device") that contained FDIC Confidential Information.

4. Since my departure from the FDIC, I have not disseminated or copied any FDIC Confidential Information from the Western Digital Device and no longer have in my possession, custody or control any FDIC Confidential Information in any format.

I declare that the foregoing statement is true and correct.

[redacted]



**Former Employees' Statements**  
**Employee-A**

---

**DECLARATION OF** [redacted]

1. My name is [redacted] I am over 18 years of age.

2. I was employed by the Federal Deposit Insurance Corporation ("FDIC") from [redacted] until I resigned effective October 23, 2015.

3. As an employee of the FDIC, I was obligated to protect FDIC confidential information, along with non-public bank supervisory information and personally identifiable information, from unauthorized disclosure ("Confidential Information"). This obligation extended beyond the termination of my employment with the FDIC.

4. On [redacted] I signed an FDIC Employee Certification and Acknowledgement of Standards of Conduct Regulation certifying that:

I have been advised that pursuant to Federal Statutes and regulations...I am prohibited from disclosing, without proper authorization, confidential personal, commercial or financial information that I have access to in my official FDIC capacity. Because these statutes carry administrative, civil or criminal penalties for the unauthorized disclosure of information, I understand that I need to contact my supervisor regarding any questions I may have about whether information may be disclosed.

5. On September 30 and October 1, 2015, while I was employed by the FDIC, I downloaded numerous files which also included Confidential Information to a non-FDIC owned external device. The files containing this Confidential Information was downloaded to a Kingston external drive, [redacted] ("Kingston Device"). I took the Kingston Device with me after my last day of work at the FDIC, at which point in time the device contained the Confidential Information that I had transferred to it. The Confidential Information was accessible to me only by virtue of my FDIC employment.

**Former Employees' Statements**  
**Employee-A**

6. Upon receiving a letter from the FDIC dated January 15, 2016 regarding my copying of Confidential Information, I delivered the Kingston Device, on January 21, 2016, to [redacted] of the FDIC, along with a second Kingston thumb drive.

7. The Kingston Device remained in my possession from my last day of employment at the FDIC until January 21, 2016, when I delivered it to the FDIC. During the time that it was in my possession, I did not make any electronic copies of the Kingston Device, nor did I copy any Confidential Information from the Kingston Device onto another computer or electronic storage device. Furthermore, I did not upload or disseminate any Confidential Information from the Kingston Device to the internet or any cloud-based storage medium. Finally, I did not print out any hard copies of Confidential Information from the Kingston Device.

8. I no longer have in my possession, custody, or control any hard copies of documents containing FDIC Confidential Information.

9. I will not disclose any FDIC Confidential Information for any purpose.

10. I agree to refrain from any and all unauthorized disclosure of FDIC Confidential Information including, but not limited to, publication on the internet.

11. If I have knowingly made any false statement, or if I breach any of the representations in this declaration, the FDIC shall be entitled to injunctive relief from any court with jurisdiction, and such relief shall be in addition to other remedies available to the FDIC under the law and/or applicable criminal penalties. Additionally, the FDIC shall be entitled to recover reasonable costs and attorney fees in connection with obtaining such injunctive relief.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: FEBRUARY 25, 2016

[redacted signature box]

**Former Employees' Statements**  
**Employee-B**



Federal Deposit Insurance Corporation

February 19, 2016

Dear [redacted]

This follows up on our numerous conversations regarding certain Federal Deposit Insurance Corporation ("FDIC") confidential information ("Confidential Information") that was in your possession after your departure from FDIC employment. We realize that departing employees sometimes leave with Confidential Information inadvertently included among their personal information and possessions, and we appreciate your acting quickly to provide to us the 120 GB SimpleTech Portable USB Disk Drive [redacted] case, instructional book and disk, and wire adapter ("Device") containing the Confidential Information.

We plan to sanitize the Device to remove all FDIC information that may have been stored on it. Please inform Supervisory Examiner [redacted] at [redacted] no later than March 15, 2016, if you would like us to return the Device to you after we have removed all information from it; if I have not heard from you by that date we will dispose of the Device.

Given the sensitive nature of the Confidential Information, we need to obtain some additional information before we can close our file on this matter. Specifically, we want to find out from you:

- Whether the Confidential Information might have been stored somewhere other than on the Device itself, from the time that it was removed from the FDIC to the time you provided the Device to us (and if so, where);  
\_\_\_ Yes  No
- The identity of any persons who had (or may have had) access to the Confidential Information during that period of time; Name: None
- Whether the Confidential Information was accessed, copied, downloaded or disseminated in any way from the time it was removed from the FDIC until the time you returned it to the FDIC's possession on November 30, 2015; \_\_\_ Yes  No; and
- Your commitment to refrain from further access to or any disclosure of the Confidential Information.  Agree \_\_\_ Disagree

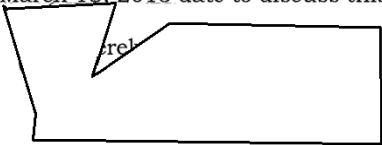
Signed [redacted]

Date: 2/19/2016

**Former Employees' Statements**  
**Employee-B**

If you downloaded or otherwise copied the Confidential Information from the Device, we will work with you to ensure that the Confidential Information is safely deleted wherever else it may be.

To facilitate your response, we could, if you wish, arrange to speak with you by telephone to obtain the necessary information described above, after which we could send you a confirming e-mail for your review. Please contact Supervisory Examiner [redacted] by March 15, 2016 date to discuss this matter.



Former Employees' Statements  
Employee-C

March 8, 2016

By Electronic Mail via [redacted]

[redacted]  
Senior Counsel  
Federal Deposit Insurance Corporation  
3501 Fairfax Dr.  
Arlington, VA 22226

Re: Download of Confidential FDIC Information

[redacted]

This letter is written in response to the letter received via email on March 7, 2016. I would like the record to reflect that I provided the one personal USB drive to [redacted] on the morning of Friday, December 11, 2015, less than 24 hours after speaking with [redacted] regarding this matter. I had offered and was willing to bring him the device during the evening we first spoke, Thursday, December 10, 2015. I understood the request was to provide any files that I had in my possession from the transfer of information.

I had personally destroyed the Seagate drive after transferring the files onto the one personal USB drive that was turned over to the FDIC. The Seagate drive, along with other electronic devices, was taken to [redacted] I was not provided with a receipt from the hardware disposal facility, so I am unable to provide you with a copy of that receipt, nor do I have the date of that drop-off. I contacted [redacted] this morning, spoke to [redacted] and was told that any devices that were dropped-off to their facility during this time period would have been destroyed and no longer in their possession.

Apart from the one personal USB drive that I provided to the FDIC, I do not have in any format, in my possession, custody, or control any additional Confidential Information. No other personal devices were used to transfer, store, or manipulate the Confidential Information.

I am also hopeful that this matter can be resolved without the need for further action beyond that outlined in your letter. If you have any further questions, please feel free to contact me at [redacted]

[redacted]

Sincerely

[redacted]

**Former Employees' Statements**  
**Employee-D**

Receipt for USB Storage Devices

Today, January 13, 2016, I delivered the following USB storage devices to the FDIC [redacted]  
[redacted]

[redacted]  
[redacted]

When FDIC is done with the devices, I would like them returned to me at the following address:

Name: [redacted]  
Street Address: [redacted]  
City, State Zip: [redacted]

If FDIC has questions about the USB storage devices, I want them to contact me at the following number:

Telephone: [redacted]

Acknowledgements

[redacted] Signature and Date: [redacted] 01/13/2015.

Received by [redacted] Supervisory Examiner, and Date: \_\_\_\_\_

Certification

I, [redacted] certify that I had the above USB storage devices in my possession the entire time period between November 1, 2015, and January 13, 2016. They were locked in a safe at my [redacted] residence. Any information on the USB storage devices was solely in my possession and was not disseminated in any way. I certify that the materials downloaded from my FDIC laptop to these USB storage devices were erased by me sometime in late December 2015.

[redacted] Signature and Date: [redacted] 01/13/2015.

Former Employees' Statements  
Employee-E



[Redacted] [Redacted]

February 19, 2016

[Redacted]

Dear [Redacted]

This follows up on our Friday, January 8, 2016, telephone call and subsequent meeting in the [Redacted] regarding certain Federal Deposit Insurance Corporation ("FDIC") confidential information ("Confidential Information") that was in your possession after your departure from FDIC employment. We appreciate your acting quickly to provide to us the two thumb drives ("Devices") described below.

- [Redacted]
- [Redacted]

Given the sensitive nature of the Confidential Information these devices may have contained, we need to obtain and document some additional information before we can close our file on this matter. Specifically, we want to find out from you:

- Whether the Confidential Information might have been stored somewhere other than on these Devices themselves, from the time that they were removed from the FDIC to the time you provided the Devices to us (and if so, where);

Yes [ ] or No [ x ] If Yes, locale: \_\_\_\_\_

- The identity of any persons who had (or may have had) access to the Confidential Information during that period of time;

Name, Name(s), or Not Applicable: Not Applicable

- Whether the Confidential Information had been accessed, copied, downloaded or disseminated in any way from the time it was removed from the FDIC until the time you returned it to the FDIC's possession on January 8, 2016;

Yes [ ] or No [ x ] If Yes, please describe: \_\_\_\_\_

## Former Employees' Statements Employee-E

[Redacted]

2 of 2

February 19, 2016

And,

- Your commitment to refrain from further access to or any disclosure of the Confidential Information.

Yes, I will refrain from further access to or any disclosure of the Confidential Information, or

No, I will not refrain from further access to or any disclosure of the Confidential Information.

If you did download or otherwise copy the Confidential Information from the Devices, we would want to work with you to ensure that the Confidential Information is safely deleted wherever else it may be. We would ask you to correspond with Supervisory Examiner [Redacted] as our point of contact in this regard.

In closing, please help us close out this matter by reviewing information above, providing requested information, and then certifying and attesting to the information provided and actions requested by signing the certification line below. Additionally, in our plan to close out this matter, we will be sanitizing the Devices to remove all information that may have been stored on them. We appreciate your assistance in this matter.

Sincerely,

[Redacted Signature]

Supervisory Examiner

Certification Statement

[Redacted Signature]

2/19/2016

Date



Former Employees' Statements  
Employee-F

---

April 11, 2016

[Redacted]  
Chief, Resource Management  
FDIC

Dear [Redacted]

I am responding to your letter dated April 11, 2016, regarding the Confidential Information contained on a hard drive device ("Device") in my possession at the time of my separation from the FDIC on February 26, 2016.

The Confidential Information was only stored on the Device, from the time that it was removed from the FDIC to the time I provided the Device to you on March 1, 2016.

There were no other individuals who had access to the Confidential Information during that period of time.

The Confidential Information was not accessed, copied, downloaded or disseminated in any way from the time it was removed from the FDIC until the time I returned the Device to the FDIC on March 1, 2016.

You have my commitment to refrain from further access to or any disclosure of the Confidential Information.

Sincerely,

[Redacted Signature]

Letters Reporting Seven "Major Incidents" to the SST Committee

  
MARTIN J. GRUENBERG  
CHAIRMAN

FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

February 26, 2016

Honorable Lamar S. Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed, please find a report prepared by the FDIC's Chief Information Officer in accordance with provisions of Public Law 113-283, the Federal Information Security Modernization Act of 2014 and OMB Memorandum M-16-03.

If you have further questions or comments, please contact me at [redacted] or Andy Jiminez, Director of the Office of Legislative Affairs, at [redacted].

Sincerely,

[redacted signature box]

Martin J. Gruenberg

Enclosure

cc: Honorable Eddie Bernice Johnson, Ranking Member

## Letters Reporting Seven “Major Incidents” to the SST Committee



**Federal Deposit Insurance Corporation**  
550 17<sup>th</sup> Street NW, Washington, D.C. 20429

February 26, 2016

**MEMORANDUM TO:** Martin J. Gruenberg  
Chairman

**FROM:** Lawrence Gross, Jr., Chief Inform[redacted] Officer and Chief Privacy Officer

**SUBJECT:** FDIC Security Incident CINC-221387


The purpose of this memorandum is to inform you of facts and circumstances related to the above referenced security incident.

Prior to separation from FDIC employment, an agency employee copied a combination of personal information along with sensitive FDIC information that the employee was authorized to access to a personally owned portable storage device. This person left FDIC employment on October 15, 2015, taking this device with them. The FDIC became aware of the incident on October 23, 2015 and referred the matter to the FDIC’s Office of Inspector General (OIG) for further investigation on November 2, 2015. On November 24, 2015, the OIG declined involvement in the matter. Through subsequent efforts by the FDIC legal division, the device was recovered from the employee on December 8, 2015.

The sensitive information on the device included customer data for over 10,000 individuals that the employee had legitimate access to for bank examination purposes while employed by the FDIC. The FDIC’s investigation does not indicate that any sensitive information has been disseminated or compromised. Evidence suggests that the sensitive information was downloaded inadvertently and without malicious intent. The FDIC’s relationship with the employee has not been adversarial, and the individual has indicated that they would be willing to sign an affidavit attesting to the fact that the information has not been further disseminated or compromised.

A review of the incident by the Office of Inspector General conveyed on February 19, 2016 indicated that reasonable grounds existed to designate the incident as a “major” incident and report it to Congress consistent with the Federal Information Security Modernization Act of 2014, Pub. Law No. 113-283 and guidance promulgated by the Office of Management and Budget in Memorandum M-16-03 dated October 30, 2015.

Letters Reporting Seven "Major Incidents" to the SST Committee

  
MARTIN J. GRUENBERG  
CHAIRMAN

FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

March 18, 2016

Honorable Lamar S. Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed, please find a report prepared by the FDIC's Chief Information Officer in accordance with provisions of Public Law 113-283, the Federal Information Security Modernization Act of 2014 and OMB Memorandum M-16-03.

If you have further questions or comments, please contact me at [redacted] or Andy Jiminez, Director of the Office of Legislative Affairs, at [redacted].

Sincerely,

[redacted signature box]

Martin J. Gruenberg

Enclosure

cc: Honorable Eddie Bernice Johnson, Ranking Member

## Letters Reporting Seven "Major Incidents" to the SST Committee

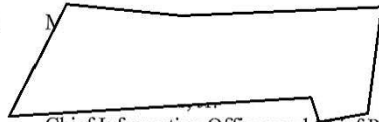


Federal Deposit Insurance Corporation  
550 17<sup>th</sup> Street NW, Washington, D.C. 20429

March 18, 2016

MEMORANDUM TO:

FROM:



Chief Information Officer and Chief Privacy Officer

SUBJECT:

FDIC Security Incident #224983

The purpose of this memorandum is to inform you of the facts and circumstances related to the above referenced security incident.

Prior to separation from FDIC employment, an agency employee copied a combination of personal information along with sensitive FDIC information that the employee was authorized to access to a personally owned, portable storage device. This person left FDIC employment on February 26, 2016, taking the device with them. The FDIC became aware of the incident on February 29, 2016, and recovered the device on March 1, 2016.

The sensitive information on the device included customer data for over 44,000 individuals that the employee had legitimate access to for bank resolution and receivership purposes while employed by the FDIC. The FDIC's investigation does not indicate that any sensitive information has been disseminated or compromised.

Evidence suggests that the sensitive information was downloaded by the individual inadvertently and without malicious intent. The FDIC's relationship with the employee has not been adversarial, and the Legal Division is coordinating the drafting of an affidavit to be sent to the former employee so that the former employee may attest to the fact that the information has not been further disseminated or compromised.

Due to the number of records involved and out of an abundance of caution, it is recommended the incident be reported to Congress as a "major" incident under the Federal Information Security Modernization Act of 2014, Pub. Law No. 113-283, and guidance promulgated by the Office of Management and Budget in Memorandum M-16-03 dated October 30, 2015.

Letters Reporting Seven "Major Incidents" to the SST Committee



FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG  
CHAIRMAN

May 9, 2016

Honorable Lamar S. Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find a report prepared by the FDIC's Chief Information Officer in accordance with provisions of Public Law 113-283, the Federal Information Security Modernization Act of 2014 and OMB Memorandum M-16-03.

If you have further questions or comments, please contact me at [redacted] or Andy Jimenez, Director of the Office of Legislative Affairs, at [redacted].

Sincerely,

[redacted signature]

Martin J. Gruenberg [redacted]

Enclosure

cc: Honorable Eddie Bernice Johnson, Ranking Member

## Letters Reporting Seven “Major Incidents” to the SST Committee



**Federal Deposit Insurance Corporation**  
550 17th Street NW, Washington, D.C. 20429-9990

May 9, 2016

MEMORANDUM TO:

Mr. J. Gruenberg  
German

FROM:

Lawrence Gross, Jr.  
Chief Information Officer and Chief Privacy Officer

SUBJECT:

Retroactive Review of FDIC Security Incidents Using Criteria  
Established by the Office of Inspector General

On October 30, 2015, the Office of Management and Budget published Memorandum M-16-03, which for the first time identified criteria for federal agencies to consider in determining whether a ‘major’ incident has occurred that should be reported to Congress under the Federal Information Security Modernization, Act of 2014, Public Law 113-283 (FISMA 2014). On February 19, 2016, the FDIC Office of Inspector General (OIG) conveyed that, based upon their interpretation of the OMB memorandum, they believed reasonable grounds existed to designate a particular prior incident as a ‘major’ incident. Part of the basis for the OIG’s conclusion was that the number of records potentially exposed exceeded 10,000 and the records were beyond FDIC control for any period of time, even if the exposure was for a short period of time and judged to be low risk.

In light of the OIG’s recommendation, the Chief Information Officer Organization took proactive steps to review all incidents that have occurred since the issuance of the OMB memorandum. The purpose of this memorandum is to inform you that we have identified five additional incidents that we believe should be considered for reporting under the new interpretation articulated by the OIG in February 2016.

### **Incident # 224419**

Prior to retirement from the FDIC, an agency employee copied a combination of personal information along with sensitive FDIC information to two personally-owned, portable storage devices. The employee took the devices with them after their last working day on December 11, 2015. The individual officially retired from FDIC employment on December 31, 2015. The FDIC became aware of the incident on January 8, 2016, with an initial estimate indicating that approximately 2,000 sensitive records were involved in the incident. The devices were recovered from the retired employee on January 13, 2016.

## Letters Reporting Seven “Major Incidents” to the SST Committee

The FDIC’s relationship with the individual has not been adversarial and evidence suggests that the sensitive information was downloaded inadvertently and without malicious intent. The retired employee signed a certification statement attesting to the fact that the files had been in their sole possession the entire time, were locked in a safe, and were not disseminated in any way.

The FDIC’s Data Breach Management Team, convened on February 26, 2016, recommended a more detailed review of the data involved. A detailed forensic review of the data, which is still ongoing, indicated on April 27, 2016 that the sensitive information on the device included customer data for over 15,000 individuals that the employee had legitimate access to while employed by the FDIC. Due to the number of records involved and consistent with the OIG’s interpretation of OMB Memorandum M-16-03, it is recommended that the incident be reported to Congress as a potential ‘major’ incident.

### **Incident # 221838**

Prior to retirement from the FDIC, an agency employee copied a combination of personal information along with sensitive FDIC information to a personally-owned, portable storage device. The individual took the device with them after their retirement from FDIC employment on October 30, 2015. The FDIC became aware of the incident on November 10, 2015, with an initial estimate indicating that approximately 1,200 sensitive records were involved in the incident. The device was recovered from the retired employee on December 3, 2015.

The FDIC’s relationship with the employee has not been adversarial and evidence suggests that the sensitive information was downloaded inadvertently and without malicious intent. The retired employee signed a certification statement attesting to the fact that the data had been in their sole possession the entire time and were not disseminated in any way.

The FDIC’s Data Breach Management Team, convened on February 26, 2016, recommended a more detailed review of the data involved. A detailed forensic review of the data, which is still ongoing, indicated on April 27, 2016 that the sensitive information on the device included customer data for over 13,000 individuals that the employee had legitimate access to while employed by the FDIC. Due to the number of records involved and consistent with the OIG’s interpretation of OMB Memorandum M-16-03, it is recommended that the incident be reported to Congress as a potential ‘major’ incident.

### **Incident # 222249**

Prior to retirement from the FDIC, an agency employee copied a combination of personal information along with sensitive FDIC information to a personal portable storage device. This person left FDIC employment on November 27, 2015 taking the device with them. The FDIC became aware of the incident on December 10, 2015, and immediately took action to retrieve the device.



## Letters Reporting Seven “Major Incidents” to the SST Committee

Through subsequent communications with the former employee, and through our own analysis, it was determined that the original storage device detected could not be returned because it had been destroyed. Additionally, the employee acknowledged having copied the information from the original device to an additional device that was subsequently returned to the FDIC. The former employee indicated that they destroyed the original device at a hardware disposal company. The former employee was unable to provide a receipt verifying the destruction of the original device but provided a signed statement attesting to the fact that the information had not been disseminated or compromised, and that the original device was in fact destroyed by a hardware disposal company. The former employee signed and returned the affidavit to the FDIC on March 8, 2016.

The sensitive information in question included customer data for over 49,000 individuals that the employee had legitimate access to while employed by the FDIC. The FDIC's investigation does not indicate that any sensitive information has been disseminated or compromised. Further, evidence indicates that the sensitive information was downloaded by the individual inadvertently while attempting to remove personal information and without malicious intent. However, due to the number of records involved and consistent with the OIG's interpretation of OMB Memorandum M-16-03, it is recommended that the incident be reported to Congress as a potential 'major' incident.

### **Incident # 224326**

Prior to retirement from FDIC employment, an agency employee copied a combination of personal information along with sensitive FDIC information to three portable storage devices. The individual took the devices with them after their retirement from FDIC employment on December 31, 2015. The FDIC became aware of the incident on January 7, 2016, with an initial estimate indicating that approximately 3,000 sensitive records were involved in the incident. The device was recovered from the retired employee on January 8, 2016.

The FDIC's relationship with the employee has not been adversarial and evidence suggests that the sensitive information was downloaded inadvertently and without malicious intent. The retired employee signed a certification statement attesting to the fact that the data had been in their sole possession the entire time and were not disseminated in any way.

The FDIC's Data Breach Management Team, convened on February 26, 2016, recommended a more detailed review of the data involved. A detailed forensic review of the data, which is still ongoing, indicated on April 29, 2016 that the sensitive information on the device included customer data for over 18,000 individuals that the employee had legitimate access to while employed by the FDIC. Due to the number of records involved and consistent with the OIG's interpretation of OMB Memorandum M-16-03, it is recommended that the incident be reported to Congress as a potential 'major' incident.

## Letters Reporting Seven “Major Incidents” to the SST Committee

---

**Incident # 221804**

Prior to separating from FDIC employment for personal reasons, an agency employee copied a combination of personal information along with sensitive FDIC information to a portable storage device. The individual took the device with them after their separation from FDIC employment on October 23, 2015. The FDIC became aware of the incident on November 10, 2015 with an initial estimate indicating that approximately 500 sensitive records were involved in the incident. The device was recovered from the former employee on January 21, 2016.

The FDIC’s relationship with the employee has not been adversarial and evidence suggests that the sensitive information was downloaded inadvertently and without malicious intent. The former employee signed a certification statement attesting to the fact that the data had been in their sole possession the entire time and were not disseminated in any way.

The FDIC’s Data Breach Management Team, convened on February 26, 2016, recommended a more detailed review of the data involved. The subsequent review of the data, which is still ongoing, indicated on May 5, 2016 that the sensitive information on the device may include customer data for over 10,000 individuals that the employee had legitimate access to while employed by the FDIC. While we have not completed our review of the data, it is recommended that this incident be reported to Congress as a ‘major’ incident out of an abundance of caution in the event our review reveals that the number of customer records exceeds 10,000.

**The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's  
April 22, 2016 Response**

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 8, 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 conducting oversight of a recent security event at the Federal Deposit Insurance Corporation (FDIC). Recently, the FDIC wrote to the Committee informing it of a security breach involving an employee who obtained sensitive data for 44,000 individuals prior to separating from employment at the agency.<sup>1</sup> Although the information was apparently downloaded from an agency database inadvertently, the Committee remains concerned about the handling of sensitive agency information and wants to ensure that the FDIC has proper controls in place to prevent further incidents. To assist in the Committee's oversight of this matter, I am writing to request a briefing and information related to the incident.

The Federal Information Security Modernization Act of 2014 (FISMA) directs Executive Branch departments and agencies to report "major" security incidents to Congress within seven days.<sup>2</sup> Because the incident met the Office of Management and Budget's guidelines for classifying an incident as a "major" security breach,<sup>3</sup> the FDIC provided a March 18, 2016 letter and report to the Committee, explaining a recent security incident.<sup>4</sup>

Earlier this year, an FDIC employee who was in the process of separating from agency employment copied personal information onto a personal portable storage device. In the process of loading information onto the storage device, the employee copied sensitive customer data for over 44,000 individuals.<sup>5</sup> When the employee left the FDIC on February 26, 2016, the employee

<sup>1</sup> Letter from Hon. Martin J. Gruenberg, Chairman, Fed. Deposit Insurance Corp., to Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech. (Mar. 18, 2016) [hereinafter Letter, Mar. 18, 2016].

<sup>2</sup> Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

<sup>3</sup> 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. 8, 2016).

<sup>4</sup> Letter, Mar. 18, 2016, *supra* note 1.

<sup>5</sup> *Id.*

## The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's April 22, 2016 Response

The Honorable Martin J. Gruenberg  
April 8, 2016  
Page 2

took the storage device from the premises.<sup>6</sup> Upon learning of the incident three days later, FDIC personnel worked to recover the device.<sup>7</sup> The device was ultimately recovered on March 1, 2016.<sup>8</sup>

As you know, sensitive information that is housed for any length of time without proper measures in place to mitigate cybersecurity risks is susceptible to a breach. Even more troubling, the potential for a breach is especially heightened when sensitive information for over 44,000 individuals is stored without proper security measures. The Committee, therefore, wants to ensure that the FDIC is taking appropriate action to mitigate the risks posed by the security incident, as well as any future cybersecurity risks, in accordance with federal information security requirements.

To assist in the Committee's oversight of the FDIC's response to the security incident, please contact Committee staff by April 15, 2016 to arrange a briefing on the matter. Please also provide the following documents and information as soon as possible, but by no later than noon on April 22, 2016. Unless otherwise noted, please provide the requested information for the time frame from January 1, 2016 to the present:

1. All documents and communications referring or relating to the security incident.
2. A detailed description of the sensitive information copied onto the former FDIC employee's portable storage device.
3. A detailed description of all major security breaches involving FDIC information for the time frame from January 1, 2009 to the present.
4. All documents and communications referring or relating to the FDIC's policies and procedures with respect to safeguarding and handling sensitive information housed on FDIC computer systems.
5. An organizational chart for the Office of the Chief Information Officer and the Office of the Chief Information Security Officer.

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 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.

---

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

**The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's  
April 22, 2016 Response**

---

The Honorable Martin J. Gruenberg  
April 8, 2016  
Page 3

If you have any questions about this request, please contact [redacted]  
[redacted] Thank you for your attention to this matter.

Sincerely,

[redacted signature]

Lamar Smith  
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

Enclosure

**The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's  
April 22, 2016 Response**

---

**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.

**The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's  
April 22, 2016 Response**

---

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 January 1, 2016 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

## The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's April 22, 2016 Response

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.



**The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's  
April 22, 2016 Response**

---

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.

## The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's April 22, 2016 Response



**Federal Deposit Insurance Corporation**  
550 17th Street NW, Washington, DC 20429

Office of Legislative Affairs

April 22, 2016

Honorable Lamar Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Smith:

This is in response to your correspondence dated April 8, 2016, requesting that the Federal Deposit Insurance Corporation produce certain documents related to a major security breach involving a former FDIC employee which we reported to the Committee on March 18, 2016.

In your letter, you also asked that the FDIC provide your staff with a briefing on the FDIC's response to the security incident. The briefing was conducted on Thursday, April 21, 2016. At the briefing, the FDIC staff explained that it carefully examines such incidents to determine any potential impact on the FDIC, affected individuals or entities.

Your April 8 letter also requested documents and communications referring or relating to the March 18 security incident report. The enclosed DVD provides documents that have been identified as responsive to your request.

The Bates range for the documents on the enclosed DVD is FDICSSST0000001 – FDICSSST0000118. The enclosed DVD has been encrypted. The password for the DVD will be transmitted to your staff by separate email. If necessary, the FDIC can provide a technical specialist to assist the Committee with accessing the documents.

Please be advised that some of the materials produced today contain both personally identifiable information (PII) and sensitive information (SI) about open and operating financial institutions. Any information regarding open and operating financial institutions as well as personally identifiable information of bank customers, employees, and other third parties has been redacted. The names of FDIC personnel serving below the level of Director and all signatures have also been redacted.

For documents that the FDIC is providing to the Committee, the FDIC has clearly marked those documents that it considers privileged or confidential. The FDIC does not believe that this or any future production of documents to the Committee affects a waiver of any privileges that may apply. For example, some of the documents may have been generated in connection with the FDIC's decision-making process and are thus protected by the deliberative process privilege. Some documents may contain confidential attorney-client communications protected by the attorney-client privilege. Moreover, apart from privileges applicable to the FDIC, some of the information produced today may include privileged information belonging to third-parties including financial institutions. Production by the FDIC of any such third-party information

**The SST Committee's April 8, 2016 Letter to the FDIC and the FDIC's  
April 22, 2016 Response**

should not be construed as a waiver of any applicable privileges. The FDIC respectfully requests that the Committee respect all applicable privileges and the confidentiality of the information contained in the documents.

In addition, the FDIC respectfully requests that the Committee give prior notice to the FDIC of any proposed release by the Committee of any non-public information contained in any of the documents that the FDIC is providing pursuant to the Committee's request. Due to the highly confidential nature of some of the materials being provided, the FDIC requests that at the conclusion of its investigation, the Committee dispose of the materials in a manner that preserves their confidentiality or return the materials to the FDIC.

Finally, the FDIC acknowledges the Committee's informal follow-up request of April 21 for additional information. We are working to identify responsive documents that will be provided in a subsequent production.

If you or Committee staff has any questions, please contact me at [redacted] or [redacted]  
[redacted]

Sincerely,

[redacted]

M. Andy Jiminez  
Director  
Office of Legislative Affairs

Enclosure: DVD

cc: Honorable Eddie Bernice Johnson, Ranking Member

**The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's  
May 4, 2016 Response**

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](http://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).<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup> On October 15, 2015, the individual officially separated from the FDIC and removed the portable storage device from FDIC premises.<sup>5</sup> Eight days later, the FDIC became aware of the incident and on November 2, 2015, referred the matter to the OIG.<sup>6</sup> The FDIC worked to recover the device and ultimately took possession of the device on December 8, 2015.<sup>7</sup>

<sup>1</sup> 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].

<sup>2</sup> 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].

<sup>3</sup> *Id.*; Letter, Apr. 8, 2016, *supra* note 1.

<sup>4</sup> Letter, Feb. 26, 2016, *supra* note 2.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

## The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's May 4, 2016 Response

The Honorable Martin J. Gruenberg  
April 20, 2016  
Page 2

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.<sup>8</sup> 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.<sup>9</sup> 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.

<sup>8</sup> *Id.*

<sup>9</sup> 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).

**The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's  
May 4, 2016 Response**

---

The Honorable Martin J. Gruenberg  
April 20, 2016  
Page 3

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 [redacted]  
[redacted]. Thank you for your attention to this matter.

Sincerely,

[redacted]

Lamar Smith  
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Minority Member

Enclosure

## The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's May 4, 2016 Response

---

### 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.

**The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's  
May 4, 2016 Response**

---

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



## The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's May 4, 2016 Response

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.

**The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's  
May 4, 2016 Response**

---

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.

**The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's  
May 4, 2016 Response**



**Federal Deposit Insurance Corporation**  
550 17th Street NW, Washington, DC 20429

Office of Legislative Affairs

May 4, 2016

Honorable Lamar Smith  
Chairman  
Committee on Science, Space & Technology  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Smith:

This is in response to your April 20, 2016 letter requesting that the Federal Deposit Insurance Corporation produce certain documents related to a major security breach involving a former FDIC employee which we reported to the Committee on February 26, 2016.

Your April 20 letter requested documents and communications referring or relating to the February 26 security incident report. The enclosed DVD provides documents that have been identified as responsive to your request.

The Bates range for the documents on the enclosed DVD is FDICSSTT0000001 – FDICSSTT0000088. The enclosed DVD has been encrypted. The password for the DVD will be transmitted to your staff by separate email. If necessary, the FDIC can provide a technical specialist to assist the Committee with accessing the documents.

Please be advised that some of the materials produced today contain both personally identifiable information (PII) and sensitive information (SI) about financial institutions. Any sensitive information regarding financial institutions as well as personally identifiable information of bank customers, employees, and other third parties has been redacted. The names of FDIC personnel serving below the level of Director and all signatures have also been redacted.

For documents that the FDIC is providing to the Committee, the FDIC has clearly marked those documents that it considers privileged or confidential. The FDIC does not believe that this or any future production of documents to the Committee affects a waiver of any privileges that may apply. For example, some of the documents may have been generated in connection with the FDIC's decision-making process and are thus protected by the deliberative process privilege. Some documents may contain confidential attorney-client communications protected by the attorney-client privilege. Moreover, apart from privileges applicable to the FDIC, some of the information produced today may include privileged information belonging to third-parties including financial institutions. Production by the FDIC of any such third-party information should not be construed as a waiver of any applicable privileges. The FDIC respectfully requests that the Committee respect all applicable privileges and the confidentiality of the information contained in the documents.

In addition, the FDIC respectfully requests that the Committee give prior notice to the FDIC of any proposed release by the Committee of any non-public information contained in any of the

**The SST Committee's April 20, 2016 Letter to the FDIC and the FDIC's  
May 4, 2016 Response**

---

documents that the FDIC is providing pursuant to the Committee's request. Due to the highly confidential nature of some of the materials being provided, the FDIC requests that at the conclusion of its investigation, the Committee dispose of the materials in a manner that preserves their confidentiality or return the materials to the FDIC.

If you or Committee staff has any questions, please contact me at [redacted] or [redacted]  
[redacted]

Sincerely,

[redacted]

M. Andy Jiminez  
Director  
Office of Legislative Affairs

Enclosure: DVD

cc: Honorable Eddie Bernice Johnson, Ranking Member

**The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's  
May 25, 2016 Response**

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 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,<sup>1</sup> and April 20, 2016.<sup>2</sup> 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.<sup>3</sup>

<sup>1</sup> 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].

<sup>2</sup> 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].

<sup>3</sup> 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 SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 2

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.<sup>4</sup> 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.<sup>5</sup>

[...]

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

**Mr. Gross:** I did—

**Rep. Loudermilk:** --provided—

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

<sup>5</sup> *Id.*

## The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 3

**Mr. Gross:** I did a cursory review.<sup>6</sup>

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.<sup>7</sup> **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.<sup>8</sup>

**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.<sup>9</sup> Mr. Loudermilk questioned Mr.

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> See E-mail from Christopher J. Farrow, to Lawrence Gross & [REDACTED] (Nov. 30, 2015, 6:33 p.m.).

## The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 4

Gross about why the agency withheld the document.<sup>10</sup> In response, Mr. Gross stated that the e-mail was summarized in materials provided to the Committee.<sup>11</sup> 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.<sup>12</sup>

**Despite the Committee's request for "all documents and communications referring or relating to the October 2015 security incident,"<sup>13</sup> 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,<sup>14</sup> 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.

<sup>10</sup> FDIC Hearing, May 12, 2016, *supra* note 4.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> Letter, Apr. 20, 2016, *supra* note 2.

<sup>14</sup> FDIC Hearing, May 12, 2016, *supra* note 4.



## The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 5

### 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**."<sup>15</sup> 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.<sup>16</sup> 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.

<sup>15</sup> 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).

<sup>16</sup> Briefing by FDIC Staff, April 21, 2016.

**The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's  
May 25, 2016 Response**

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 6

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.<sup>17</sup>

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.<sup>18</sup> 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

<sup>17</sup> FDIC Hearing, May 12, 2016, *supra* note 4.

<sup>18</sup> See Letter from [redacted] Senior Counsel, FDIC to [redacted] the [redacted] Law Firm (Dec. 2, 2015) [hereinafter Letter, Dec. 2, 2015].

## The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 7

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.<sup>19</sup> 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."<sup>20</sup> **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.<sup>21</sup> Even more troublesome, Mr. Gross could not certify that the remedial actions taken could have prevented the breaches.<sup>22</sup>** 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?

<sup>19</sup> 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/>.

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

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

<sup>22</sup> *Id.*

## The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 8

**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.<sup>23</sup>

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 [redacted] 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,<sup>24</sup> 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" incidents<sup>25</sup> provide "some guidance to the agency to consider in making a determination of, one, the significance of an event."<sup>26</sup> 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

<sup>23</sup> *Id.* (emphasis added).

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

<sup>25</sup> 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).

<sup>26</sup> FDIC Hearing, May 12, 2016, *supra* note 4.

The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's  
May 25, 2016 Response

The Honorable Martin J. Gruenberg  
May 19, 2016  
Page 9

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

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 [redacted]. Thank you for your attention to this matter.

[redacted]

Lamar Smith  
Chairman

Sincerely,

[redacted]

Barry Loudermilk  
Chairman  
Subcommittee on Oversight

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

<sup>27</sup> *Id.*

## The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's May 25, 2016 Response



FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG  
CHAIRMAN

May 25, 2016

Honorable Lamar S. Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Honorable Barry Loudermilk  
Chairman  
Subcommittee on Oversight  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Smith and Chairman Loudermilk:

This is in response to your May 19, 2016 letter regarding the testimony of the FDIC's Chief Information Officer (CIO) before the House Committee on Science, Space, and Technology on May 12, 2016. I appreciate the opportunity to respond to issues raised in your letter. We look forward to reviewing the full, official hearing transcript so that additional responses may be provided as needed.

We regret that the FDIC's productions thus far in regard to the Committee's requests for documents dated April 8, 2016, and April 20, 2016, have been unsatisfactory to the Committee. We appreciate the opportunity to better meet the Committee's needs. We have initiated a broader search for additional e-mail records referencing the incidents that were reported on February 26 and March 18 and will provide the Committee with additional documents. We have reached out to Committee staff in an effort to receive feedback on search terms that are satisfactory to the Committee. Further, in response to your most recent letter dated May 24, 2016, we have initiated a new search for documents and communications, including those relating to the scope of the FDIC's responses to the Committee's requests of April 8, 2016, and April 20, 2016.

As you are aware, the FDIC has reported seven incidents as "major incidents" pursuant to the Office of Management and Budget (OMB) Guidance M-16-03, issued on October 30, 2015. The FDIC reported the incidents after the FDIC's Office of Inspector General (OIG) issued a report on February 19, 2016, recommending that an incident involving a former employee be reported to Congress as a major incident. The FDIC did so, and subsequently reported six other incidents to Congress under the major incident criteria used by the OIG. The incidents involved departing employees who had satisfactory employment records and legitimate access to the data involved. In each instance, the information was recovered and there was no evidence of further

**The SST Committee's May 19, 2016 Letter to the FDIC and the FDIC's  
May 25, 2016 Response**

---

dissemination or disclosure. In addition, the OIG did not further investigate any of the incidents. Under these circumstances, it was the initial judgment of the CIO that these incidents did not meet the definition of a major incident within the context of the Federal Information Security Modernization Act of 2014 or OMB Guidance M-16-03. However, once the OIG's recommendation was issued, the FDIC adopted the criteria used by the OIG.

These incidents highlighted the risks associated with removable media, such as DVDs, CDs, and flash drives. As a result, we are moving swiftly to discontinue the use of removable media at the FDIC. In the meantime, we have implemented software that automatically encrypts removable media to which FDIC information is downloaded.

These are matters of great consequence to the FDIC and we are committed to addressing them. We also are committed to cooperating with the Committee as it inquires into these matters.

If you have additional questions, please contact me at

Sincerely,

Martin J. Gruenberg

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

The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's  
June 20, 2016 Response

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 27, 2016

Mr. Lawrence Gross, Jr.  
CIO and CPO  
Federal Deposit Insurance Corporation  
3501 Fairfax Drive  
Arlington, VA 22226

Dear Mr. Gross:

On behalf of the Committee on Science, Space, and Technology, I want to express my appreciation for your participation in the hearing entitled *FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?* on May 12, 2016.

You have received a verbatim electronic transcript of the hearing for your review. The Committee's rule pertaining to the printing of transcripts is as follows:

*The transcripts of those hearings conducted by the Committee and Subcommittees shall be published as a substantially verbatim account of remarks actually made during the proceedings, subject only to technical, grammatical, and typographical corrections authorized by the person making the remarks involved.*

Transcript edits, if any, should be submitted no later than June 10, 2016. If no edits are received by the above date, I will presume that you have no suggested edits to the transcript.

I am also enclosing questions submitted for the record by Members of the Committee. These are questions that the Members were unable to pursue during the time allotted at the hearing, but felt were important to address as part of the official record. **It would be appreciated if you would respond to these questions by June 10, 2016.**

All transcript edits and responses to the enclosed questions should be submitted to me and directed to the attention of [redacted]. If you have any further questions or concerns, please contact [redacted].

Thank you again for your testimony.

Sincerely,

[redacted]  
Barry L. Undermink  
Chairman  
Subcommittee on Oversight



**The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's  
June 20, 2016 Response**

---

**Questions for the Record (QFRs)**

Subcommittee on Oversight  
Committee on Science, Space & Technology

Subcommittee hearing:  
*"FDIC Data Breaches:  
Can Americans Trust that Their Private Banking Information Is Secure?"*

May 12, 2016

Questions for the Record to:

- Mr. Lawrence Gross, Jr., Chief Information Officer and Chief Privacy Officer, FDIC

**Submitted by Representative Don Beyer, Ranking Member**  
Subcommittee on Oversight

**QFR for Mr. Lawrence Gross, Jr., CIO, FDIC**

- 1) OMB Memorandum M-16-03 was released on October 30, 2015, and was very new guidance when FDIC was dealing with the aftermath of the October 2015 "Florida breach." The Memorandum laid out new responsibilities, new definitions, and new Congressional reporting deadlines for agencies hit with cybersecurity breaches.
  - a. Were you briefed on OMB Memorandum M-16-03 prior to your December 8th decision that the October breach was not a "major" incident?
  - b. If so, when was this briefing, who provided the briefing, who else was in attendance, and what specifically were you told about OMB Memorandum M-16-03?
  - c. What efforts, in detail, did the FDIC CIO office take in order to understand the dictates of OMB Memorandum M-16-03?

**The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's  
June 20, 2016 Response**

---

- 2) You've stated, in multiple mediums, that part of your rationale for originally NOT declaring the October 2015 breach a "major incident" was a host of "mitigating factors, including the belief that the former employee was not disgruntled, and the Agency's relationship with the employee was not adversarial.
  - a. Why did you find these "mitigating" factors dispositive in determining whether the breach was a "major incident"?
  - b. Who, if anyone, advised you that these factors were relevant or applicable to an assessment of a "major incident," and the ensuing reporting requirements, as described in OMB Memorandum M-16-03?
- 3) Can you tell us the total number of individuals and institutions affected by all seven of the breaches discussed at the hearing?
- 4) Since the October OMB guidance has come out on major cyber incidents, has the issue Congressional Notification been discussed at the Data Breach Management Team (DBMT) meetings?
  - Have you been party to any debate at the DBMT meetings or in any other setting at FDIC regarding Congressional Notification?
- 5) Have you discussed the new OMB guidance with other CIOs at other Executive Branch Agencies and specifically the issue of Congressional notification? Please summarize when and where these discussions took place and briefly describe the context of these discussions.
- 6) In your testimony, you insinuated that not every breach with 10,000 or more affected records would trigger the 7-day Congressional notification requirement. (1698-1720) Under what authority do you make that assertion?

The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's  
June 20, 2016 Response



Federal Deposit Insurance Corporation  
560 17th Street NW, Washington, DC 20429

June 20, 2016

TRANSMITTED VIA ELECTRONIC MAIL

Honorable Barry Loudermilk  
Chairman  
Subcommittee on Oversight  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Loudermilk:

The purpose of this letter is to respond to your May 27, 2016 letter in which you provided the transcript of my May 12, 2016 testimony as well as questions from Congressman Don Beyer, Ranking Member of the Subcommittee.

I have reviewed my transcript and would like to clarify three points in my testimony, which was an accurate representation of the facts and circumstances as I recalled them at the time.

First, the Florida incident will be reported in our 2016 annual FISMA report rather than being reported in our 2015 annual FISMA report (as stated in line 802), since this incident occurred after the 2015 fiscal year end.

Second, the seven incidents reported involved four retiring individuals, two individuals whose employment terms had ended, and one individual who left FDIC employment for personal reasons. I said that I believed there were five individuals who were retiring (lines 1287-1290) and that I believed the rest were term employees.

Third, our Office of Legislative Affairs coordinated our response to your committee. I had originally stated that the Office of Legal Affairs coordinated the response (lines 736-737).

My answers to the questions for the record from Representative Don Beyer and minor technical corrections to the transcript also are enclosed.

If you have additional questions, please feel free to contact me at [redacted]  
or [redacted]

Sincerely,

Lawrence Gross, Jr.  
Chief Information Officer

cc: Honorable Don Beyer, Ranking Member

Enclosures

**The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's  
June 20, 2016 Response**

---

**Response to questions from  
the Honorable Don Beyer  
from the Federal Deposit Insurance Corporation**

**Q1: OMB Memorandum M-16-03 was released on October 30, 2015, and was very new guidance when FDIC was dealing with the aftermath of the October 2015 "Florida breach." The Memorandum laid out new responsibilities, new definitions, and new Congressional reporting deadlines for agencies hit with cybersecurity breaches.**

- a. Were you briefed on OMB Memorandum M-16-03 prior to your December 8th decision that the October breach was not a "major" incident?**
- b. If so, when was this briefing, who provided the briefing, who else was in attendance, and what specifically were you told about OMB Memorandum M-16-03?**
- c. What efforts, in detail, did the FDIC CIO office take in order to understand the dictates of OMB Memorandum M-16-03?**

Evaluating incidents in light of the new OMB Memorandum M-16-03 was an immediate task for me when I started at the FDIC on November 2, 2015. The "Florida breach" activities, which occurred in September and October 2015 prior to my arrival and before OMB Memorandum M-16-03 was published, had been discovered on October 23, 2015. On October 30, 2015, the Friday before I arrived, M-16-03 was published. Although OMB Memorandum M-16-03 was published after the "Florida breach," I thought it appropriate that we consider whether or not the "Florida breach" would rise to the level of a "major" incident under OMB Memorandum M-16-03 guidance.

Since OMB Memorandum M-16-03 had just been issued, the FDIC had not yet updated policies and procedures to be responsive. I directed the CISO to compare OMB Memorandum M-16-03 with existing FDIC policies and procedures and to identify any changes required. I asked that target dates be identified for our policy and procedure revisions to address gaps within the FDIC IT management, privacy, and IT security programs.

Our Legal Division provided a written memorandum dated November 18, 2015, with the subject line "Applicability of OMB Memorandum M-16-03: Fiscal Year 2015-2016 Guidance on Improving Federal Information Security and Privacy Management Requirements." This memorandum provided background regarding FISMA applicability to the FDIC and related reporting requirements, and provided an overview of OMB Memorandum M-16-03. It also provided a section by section analysis of the memorandum that highlighted changes from prior guidance. I read this memorandum and understood the conclusion that "M-16-03 is generally applicable to the FDIC."

I sought input from the Chief Information Security Officer (CISO) and legal staff as we gathered and analyzed facts, and took risk mitigation steps consistent with our incident

## The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's June 20, 2016 Response

handling policies and procedures in relation to the "Florida breach." Fact gathering and analysis is coordinated through a multi-disciplinary FDIC Data Breach Management Team (DBMT) that serves as an advisory body to the CIO when incidents occur. This multi-disciplinary advisory body reviews the information available to assess risk of harm to the FDIC and other entities. The DBMT also recommends actions to the CIO to mitigate the risk of harm. The DBMT met twice in November to consider the facts and recommend appropriate actions to be taken. The DBMT was cognizant of the new reporting requirements and recommended actions consistent with the guidance, such as counting the individuals whose PII was part of the incident.

Later, I also received an OIG memorandum dated February 19, 2016 with the subject line "Information Security Incident Warranting Congressional Reporting." I read the memorandum and understood the reasoning behind the OIG's interpretation of OMB Memorandum M-16-03 as it applied to the "Florida breach." We reported the "Florida breach" to Congress on February 26, 2016. I communicated to staff that we would use the OIG's interpretation going forward and in March we reported a late February incident using the OIG interpretation. In addition, we began a retroactive review of all incidents since October 30, 2015, through the present to determine if other previous incidents should be reported. We identified five additional incidents that we reported to Congress in May.

**Q2: You've stated, in multiple mediums, that part of your rationale for originally NOT declaring the October 2015 breach a "major incident" was a host of "mitigating factors," including the belief that the former employee was not disgruntled, and the Agency's relationship with the employee was not adversarial.**

**a: Why did you find these "mitigating" factors dispositive in determining whether the breach was a "major incident"?**

**b: Who, if anyone, advised you that these factors were relevant or applicable to an assessment of a "major incident," and the ensuing reporting requirements, as described in OMB Memorandum M-16-03?**

The facts surrounding the incident that were known at the time raised questions regarding whether or not the incident rose to the level of a "major" incident. In good faith, I considered, with input from the CISO and legal staff, the Federal Information Security Modernization Act of 2014 (FISMA 2014), OMB Memorandum M-16-03, and FDIC policies and procedures, which are based on NIST publications. Our intent was to follow the OMB Memorandum M-16-03 guidance, and to use FISMA 2014 and these other documents to provide context where we had questions as to OMB's intent.

I considered these mitigating factors (and others) in evaluating whether or not the breach was a major incident because I believed they were relevant to determining the risk of harm of the incident. I believed the four subparts of OMB Memorandum M-16-03's three-prong test existed to differentiate incidents where there was low risk of harm from those where there was greater risk of harm. Particularly, I believed these mitigating

## The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's June 20, 2016 Response

factors were relevant to determining whether or not the information was recoverable, and whether or not it had been exfiltrated (two incident characteristics that are relevant to determining the risk of harm). Our internal Data Breach Handling Guide also instructs the reader to differentiate incidents based on risk of harm and points the reader to incident characteristics to consider.

In retrospect, and based on the OMB guidance and facts I had at the time, I should not have placed reliance on these factors in determining whether or not the incident was "major." After receiving the OIG's February 19, 2016 memorandum, we adopted their analysis and conclusions and have since then reported consistent with it. We would now classify a similar incident as major.

**Q3: Can you tell us the total number of individuals and institutions affected by all seven of the breaches discussed at the hearing?**

Our analysis to date indicates that approximately 200,000 individuals' information was involved in these incidents related to approximately 380 financial institutions. We are now in the process of offering credit monitoring services to the individuals at no cost to them to protect any individuals who were potentially affected, and to be responsive to the concerns raised by the members of the Committee.

**Q4: Since the October OMB guidance has come out on major cyber incidents, has the issue of Congressional Notification been discussed at the Data Breach Management Team (DBMT) meetings?**

**Have you been party to any debate at the DBMT meetings or in any other settings at FDIC regarding Congressional Notification?**

I have had a number of discussions with the DBMT collectively, and some members individually, to ensure members were aware of the heightened reporting obligations under FISMA 2014 and OMB Memorandum M-16-03. I had several discussions with the CISO, legal staff, and others as new information arrived. The notes from the DBMT's November 25, 2015 meeting indicate that the CISO also informed DBMT members of the FISMA reporting requirements. Finally, we recently had discussions regarding how our internal policies and procedures should be updated to better address FISMA 2014 and OMB Memorandum M-16-03. On June 13, 2016, we released version 1.5 of the guide that contained changes to reference the new reporting requirements in FISMA 2014 and OMB Memorandum M-16-03.

**Q5: Have you discussed the new OMB guidance with other CIOs at other Executive Branch Agencies and specifically the issue of Congressional notification? Please summarize when and where these discussions took place and briefly describe the context of these discussions.**

Soon after receiving the OIG's February 19, 2016 memorandum, I had informal telephonic discussions with my counterparts at other agencies to discuss the FDIC's reporting approach under FISMA 2014 and OMB Memorandum M-16-03.

## The SST Committee's May 27, 2016 Letter to the FDIC and the FDIC's June 20, 2016 Response

---

**Q6: In your testimony, you insinuated that not every breach with 10,000 or more affected records would trigger the 7-day Congressional notification requirement. (1698-1720) Under what authority do you make that assertion?**

To clarify, although we have considered how best to update our policies and procedures to address FISMA 2014 and OMB Memorandum M-16-03, since receiving the OIG's February 19, 2016 memorandum, the FDIC has evaluated incidents consistent with the OIG's analysis and conclusions. For example, there was an incident in late February that was evaluated using the OIG's interpretation, which was reported to Congress in March. We have also reported five incidents based on a retrospective review of all incidents that occurred after October 30, 2015, but before receiving the OIG's memorandum.

OMB Memorandum M-16-03 guidance provides a three-prong test, two subparts of which specify the 10,000 or more record, or users affected count. One subpart implies that if the information in question is recoverable within a specified amount of time, and without supplemental resources, the 10,000 or more record, or users affected count, would not be applicable for that prong. In another subpart, if the incident does not involve the exfiltration, modification, deletion, unauthorized access, or lack of availability to information or systems, then that prong would not be triggered, regardless of the record, or users count.

I understand that the number of records and individuals potentially affected by an incident are significant factors in determining when to report to Congress, and also believe that there are types of incidents that should be reported before the number of records and individuals potentially affected is known, or when the number is known and under 10,000. An example would be an incident where an Advanced Persistent Threat actor is identified as having unauthorized network access, but it is not yet known whether records or individuals are affected.

The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

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.sscience.house.gov

August 1, 2016

The Honorable Martin J. Gruenberg  
Chairman  
Federal Deposit Insurance Corporation  
550 17<sup>th</sup> St, NW  
Washington, DC 20429

Dear Chairman Gruenberg:

On behalf of the Committee on Science, Space, and Technology, I want to express my appreciation for your participation in the hearing entitled *Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?* on July 14, 2016.

You have received a verbatim electronic transcript of the hearing for your review. The Committee's rule pertaining to the printing of transcripts is as follows:

*The transcripts of those hearings conducted by the Committee and Subcommittees shall be published as a substantially verbatim account of remarks actually made during the proceedings, subject only to technical, grammatical, and typographical corrections authorized by the person making the remarks involved.*

Transcript edits, if any, should be submitted no later than August 15, 2016. If no edits are received by the above date, I will presume that you have no suggested edits to the transcript.

I am also enclosing questions submitted for the record by Members of the Committee. These are questions that the Members were unable to pursue during the time allotted at the hearing, but felt were important to address as part of the official record. **It would be appreciated if you would respond to these questions by August 15, 2016.**

All transcript edits and responses to the enclosed questions should be submitted to me and directed to the attention of [redacted] If you have any further questions or concerns, please contact [redacted]

Thank you again for your testimony.

Sincerely,

[redacted signature box]

Lamar Smith  
Chairman



**The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's  
August 25, 2016 Response**

---

**QUESTIONS FOR THE RECORD  
The Honorable Mo Brooks (R-AL)  
U.S. House Committee on Science, Space, and Technology**

*Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers'  
Banking Information*

Thursday, July 14, 2016

**Questions for Mr. Gruenberg**

1. Does the FDIC employ the standard protections: full-disk encryption on all personal machines, remote management of security (not user-configured security), two-factor authentication, etc.?
2. What is the FDIC's risk management strategy?
  - a. What process does the FDIC use for evaluating the most important data to secure?
  - b. How does the FDIC information security strategy then allocate resources to accordingly protect those resources?
3. What methods have you employed to ensure that your security protections work?
  - a. Do you employ red teaming?
  - b. If you have engaged in red teaming, what were the rules? Could the red teams engage in social engineering? Did the red teams have to operate within the law in conducting the attacks against your systems?

**The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's  
August 25, 2016 Response**

---

**Questions for the Record (QFRs)  
to Mr. Martin Gruenberg, Chairman,  
Federal Deposit Insurance Corporation (FDIC)**

**From Rep. Don Beyer,  
Ranking Member,  
Subcommittee on Oversight,  
Committee on Science, Space & Technology**

**Full Committee Hearing,  
"Evaluating FDIC's Response to Major Data Breaches:  
Is the FDIC Safeguarding Consumers' Banking Information?"**

Thursday, July 14, 2016, 10:00 a.m., Rayburn 2318

**QFR #1 on 2010/2011 Advanced Persistent Threat (APT):** In 2010, FDIC's computers were penetrated by an "Advanced Persistent Threat" (APT). The FDIC Office of Inspector General (OIG) investigated this breach in a report it issued in 2013. Some of the FDIC's senior IT security officials at the time failed to inform either the IG's office or senior FDIC officials, including you, about this penetration and its significance. At the July 14 hearing you were informed that one FDIC employee testified that you were supposedly not told about this penetration at the time because of concerns regarding your confirmation hearing to become the FDIC Chairman. Please take this opportunity to more fully describe when you first became aware of the 2010/2011 cybersecurity attack, who informed you of this incident, when you became aware that this information was not shared with you and other senior FDIC officials, and what specific actions you took both procedurally and against specific personnel to hold individuals accountable and to improve FDIC's cybersecurity posture.

**The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's  
August 25, 2016 Response**

**Questions for the Record (QFRs)  
to Mr. Martin Gruenberg,  
Chairman, Federal Deposit Insurance Corporation (FDIC)**

**From Ms. Eddie Bernice Johnson,  
Ranking Member,  
Committee on Science, Space & Technology**

Full Committee Hearing,  
Committee on Science, Space & Technology:  
**"Evaluating FDIC's Response to Major Data Breaches:  
Is the FDIC Safeguarding Consumers' Banking Information?"**

Thursday, July 14, 2016, 10:00 a.m., Rayburn 2318

**QFR #1 on Digital Rights Management/Data Loss Prevention:** At the July 14 FDIC cybersecurity hearing the Majority suggested that establishing "Digital Rights Management" technologies at the Federal Deposit Insurance Corporation (FDIC) would render the Agency's use of its current Data Loss Prevention (DLP) software ineffective. Digital Rights Management (DRM) technologies generally refer to a mix of technologies that can prevent files from being copied, shared or altered. DRM software can also be used to provide a specified window of time in which a particular recipient may be granted access to certain data or files. On the other hand, DLP software is used to alert information technology (IT) security officials when particularly sensitive data is sent to an e-mail address outside an Agency or organization, printed, or downloaded to removable media, such as a thumb drive, for instance. In one of the Majority's "transcribed interviews," a FDIC cybersecurity expert made clear that DRM is "a great tool" that "would actually integrate with a data loss prevention tool." In addition, commercial IT security companies, including Symantec, Adobe and McAfee all suggest using DRM in combination with DLP software. Suggesting that employing DRM would "render DLP ineffective," does not appear to be accurate. However, there have been concerns about how FDIC will integrate these two tools together to be most effective.

**QFR #1:** Can you please indicate what steps are being taken to ensure that DRM will be integrated effectively with FDIC's DLP software and does not have the unintended consequence of diminishing FDIC's cybersecurity tools already in place.

**QFR #2 on FDIC Measures Since Reported Data Breaches:** The impetus for the first Science Committee hearing on FDIC data breaches was held on May 12, 2016 and looked at a series of breaches related to removable media and departing employees. What actions have the FDIC taken to prevent data breaches related to removable media and FDIC employees? Specifically, what actions have been taken since the first hearing—on May 12, 2016—and are other actions to enhance FDIC's cybersecurity procedures planned?

**The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's  
August 25, 2016 Response**



FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG  
CHAIRMAN

August 25, 2016

Honorable Lamar Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Smith:

Thank you for your letter enclosing questions from Members of the Committee subsequent to my testimony on "Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?" before the Committee on July 14, 2016. Enclosed are my responses to those questions.

Also, I have reviewed my transcript and would like to offer technical edits to the transcript, which are also enclosed.

If you have further questions or comments, please do not hesitate to contact me at

[redacted] or M. Andy Jiminez, Director of Legislative Affairs, at [redacted]

Sincerely,

[redacted signature box]

Martin J. Gruenberg

Enclosures

## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

**Response to questions by Congressman Mo Brooks  
from Martin J. Gruenberg,  
Chairman, Federal Deposit Insurance Corporation**

**Q1: Does the FDIC employ the standard protections: full-disk encryption on all personal machines, remote management of security (not user-configured security), two-factor authentication, etc.?**

**A1:** FDIC laptop hard drives are encrypted using a commercially-available solution that is consistent with NIST encryption standards.<sup>1</sup> FDIC desktop hard drives are not encrypted but are located within secured FDIC premises with cases that are locked such that non-authorized employees are unable to physically access the hard drives. The FDIC is evaluating the replacement of desktops with laptops.

To help protect sensitive email, the FDIC also provides email encryption solutions. One solution is used for sensitive email exchanges with parties outside the FDIC and a second solution is used to encrypt sensitive internal emails.

FDIC personal computers (PCs)<sup>2</sup> are managed by information technology administrators, not the end users. End users are limited in what they are able to change on PCs because they do not have operating system administrator privileges. PCs also have standard software configurations that are periodically updated with automated tools.

Two-factor authentication is currently required to access the FDIC network from PCs outside the FDIC network,<sup>3</sup> and in most instances to access the network internally if the individual is a privileged user. The FDIC is migrating from a physical token for two factor authentication to Personal Identification Verification (PIV) cards. Once PIV cards are deployed, the FDIC will incrementally change the environment so that PIV cards are required for FDIC employees and contractors to access FDIC information technology resources from anywhere.

Other protections and controls are deployed to FDIC's PCs such as: anti-virus, host-based intrusion prevention, data loss prevention, and application whitelisting software.

Additionally, the FDIC utilizes protections for the BlackBerry and Apple smart phones and tablets it provides to a subset of employees. Both BlackBerry and Apple devices have encrypted containers that protect FDIC sensitive information on the devices. These devices are ID and password protected and the FDIC is exploring two-factor access solutions that could be added to these devices.

---

<sup>1</sup> Federal Information Processing Standard (FIPS) Publication 140-2, common criteria EAL4.

<sup>2</sup> Personal computers refers both to laptops and desktops.

<sup>3</sup> For example, FDIC examiners connecting to the FDIC network from a commercial cellular network while working at a bank.

## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

**Q2: What is the FDIC's risk management strategy?**

- a. **What process does the FDIC use for evaluating the most important data to secure?**
- b. **How does the FDIC information security strategy then allocate resources to accordingly protect those resources?**

**A2:** The FDIC's risk management strategy is to ensure assets are well-identified and categorized, and that controls are deployed to protect assets based on their value or level of sensitivity.

The FDIC maintains asset inventories (systems, hardware, and data) and currently uses the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard 199, "Standards for Security Categorization of Federal Information and Information Systems," to categorize assets. Assets are categorized with regard to their confidentiality, integrity, and availability requirements (CIA). Additionally, the FDIC recently completed a review of our systems based on the Office of Management and Budget's (OMB) High Value Asset (HVA) definition, and provided a list of the top 18 HVA systems based on that review to the Department of Homeland Security. The FDIC is reviewing these systems and their associated business processes in light of OMB guidance to determine if additional controls are required.

When systems are created, the system hardware and data CIA ratings are evaluated to characterize the system as a whole and determine the appropriate NIST baseline controls to apply. Factors such as whether the system contains sensitive PII or sensitive business information, whether it is Internet-facing, whether it is a financial system, and whether it is mission critical also impact the security scrutiny it receives. Systems are also classified as either major or minor based on their importance to the FDIC's mission, finances, management visibility, and other impact categories. Those systems rated as major receive the most significant security scrutiny and resource allocation.

Finally, the FDIC has a continuous monitoring program based on NIST's Risk Management Framework and on NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems." The FDIC's continuous monitoring methodology consists of five essential components:

1. configuration management and change control,
2. an information security risk management program,
3. a Security Impact Analysis,
4. security status monitoring and reporting, and
5. active involvement of FDIC officials.

This five-part program produces a regularly updated inventory of information security improvement tasks that are prioritized based on risk, and completed with oversight by the Chief Information Officer (CIO).

## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

---

**Q3: What methods have you employed to ensure that your security protections work?**

**a. Do you employ red teaming?**

**b. If you have engaged in red teaming, what were the rules? Could the red teams engage in social engineering? Did the red teams have to operate within the law in conducting the attacks against your systems?**

**A3:** Yes, the FDIC contracted in both 2015 and 2016 with an independent, third-party company to perform adversary simulations ("red teaming") to identify weaknesses in its security posture.

The rules for the simulations were that the company could target any FDIC system and use any credentials they could access. Social engineering and denial of service attacks were out of scope. The testers used methods that would be illegal if they were not specified in the contract. The company exploited vulnerable systems and misused exposed credentials using methods similar to criminal hackers.

In addition, the FDIC maintains an ongoing contract with a company to regularly test both FDIC employees and contractors for susceptibility to phishing exploits. Employees and contractors who fail these tests are directed to training material to enhance their ability to spot phishing attacks in the future.

Finally, the FDIC participates in the DHS-sponsored Cyber Hygiene assessment on a weekly basis to help identify any weaknesses and improve security in Internet-facing systems.

## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

Response to questions by Congressman Don Beyer  
from Martin J. Gruenberg,  
Chairman, Federal Deposit Insurance Corporation

**Q1: In 2010, FDIC's computers were penetrated by an "Advanced Persistent Threat" (APT). The FDIC Office of Inspector General (OIG) investigated this breach in a report it issued in 2013. Some of the FDIC's senior IT security officials at the time failed to inform either the IG's office or senior FDIC officials, including you, about this penetration and its significance. At the July 14 hearing you were informed that one FDIC employee testified that you were supposedly not told about this penetration at the time because of concerns regarding your confirmation hearing to become the FDIC Chairman. Please take this opportunity to more fully describe when you first became aware of the 2010/2011 cybersecurity attack, who informed you of this incident, when you became aware that this information was not shared with you and other senior FDIC officials, and what specific actions you took both procedurally and against specific personnel to hold individuals accountable and to improve FDIC's cybersecurity posture.**

**A1:** I first became aware of the cybersecurity attack on August 26, 2011, during a briefing by our Chief Information Officer (CIO) and Division of Information Technology (DIT) director Russell Pittman, and Chief Information Security Officer (CISO) Ned Goldberg. The briefing provided a general summary of the security issue and suggested that the matter was a routine computer security event and was contained. I received no subsequent briefings on the topic until March 2013 when the FDIC Office of Inspector General (OIG) notified me that the incident had not, in fact, been contained in 2011 and that DIT had found it necessary to continue to address the intrusion since that time. The OIG conducted an investigation of the incident and provided their report to me on May 24, 2013. I learned from this report that DIT failed to fully inform me, other Board members, and the Chief Risk Officer of the severity and magnitude of the intrusion, did not report the incident in any meaningful way to US-CERT, and failed to adequately disclose the incident to the Government Accountability Office and the FDIC OIG.

In response to these events, the FDIC realigned its IT organizational structure and major functions to enhance accountability and eliminate potential conflicts among key roles. The positions of CIO and DIT director were separated, with the CIO to report directly to the Chairman, and the DIT director to the CIO. The information security and privacy unit was moved out of DIT and established as a separate entity reporting to the CIO. The CISO left the agency in 2013 and the responsibilities of the DIT director were curtailed. Finally, the FDIC established a senior-level committee chaired by the Chief Operating Officer that meets monthly to assess cyber security threats and developments impacting both the FDIC and the banking industry.

The FDIC also contracted with an outside cybersecurity firm, Mandiant, to determine if the incident was ongoing and to assist the FDIC in hardening our environment against any future attack. Mandiant delivered a report in September 2013 that concluded "no evidence of ongoing attack activity was identified during Mandiant's investigation." Due to a lack of evidence of ongoing attack activity or compromised systems, Mandiant could not tailor its remediation



## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

---

recommendations based on investigative findings. Instead, Mandiant recommended that the FDIC evaluate the feasibility of implementing a set of 23 recommendations that apply to most victims of targeted attacks.

The FDIC evaluated and began implementing 18 of the 23 items Mandiant recommended. Three of the 23 were already in place, and two could not be implemented in the FDIC environment. Eleven of the 18 recommendations the FDIC pursued have been completed, and the remaining seven required significant change and are still in process. However, material progress has been made on those seven and the FDIC has implemented mitigating controls and protections to lower risk while all necessary actions are completed.

The FDIC has improved the information security and privacy program in several ways beyond the Mandiant recommendations. For example, we have added seven permanent staff to the information security and privacy team.<sup>4</sup> We also have implemented or extended tools that help protect our sensitive information such as the Data Loss Prevention tool and a tool deployed to PCs that detects unauthorized software. We also have deployed new protective tools at our firewalls to prevent external threats from gaining access to our systems.

---

<sup>4</sup> In two of these cases, a temporary position was replaced with a permanent position.

## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

Response to questions from Congresswoman Eddie Bernice Johnson  
from Martin J. Gruenberg,  
Chairman, Federal Deposit Insurance Corporation

**Q1:** At the July 14 FDIC cybersecurity hearing the Majority suggested that establishing “Digital Rights Management” technologies at the Federal Deposit Insurance Corporation (FDIC) would render the Agency’s use of its current Data Loss Prevention (DLP) software ineffective. Digital Rights Management (DRM) technologies generally refer to a mix of technologies that can prevent files from being copied, shared or altered. DRM software can also be used to provide a specified window of time in which a particular recipient may be granted access to certain data or files. On the other hand, DLP software is used to alert information technology (IT) security officials when particularly sensitive data is sent to an e-mail address outside an Agency or organization, printed, or downloaded to removable media, such as a thumb drive, for instance. In one of the Majority’s “transcribed interviews,” a FDIC cybersecurity expert made clear that DRM is “a great tool” that “would actually integrate with a data loss prevention tool.” In addition, commercial IT security companies, including Symantec, Adobe and McAfee all suggest using DRM in combination with DLP software. Suggesting that employing DRM would “render DLP ineffective,” does not appear to be accurate. However, there have been concerns about how FDIC will integrate these two tools together to be most effective.

**Can you please indicate what steps are being taken to ensure that DRM will be integrated effectively with FDIC’s DLP software and does not have the unintended consequence of diminishing FDIC’s cybersecurity tools already in place.**

**A1:** The FDIC has researched solutions that claim to directly integrate DLP and DRM software, and researched possible FDIC integrations that could ensure DLP and DRM software function effectively, without degrading one another.

For example, makers of DLP and DRM software make claims of software integration so that DLP tools can review the contents of a DRM-wrapped file. Some of these tools are not yet on the market, but are promised soon. The FDIC has researched these solutions and how effective they may be in our environment.

Separately, the FDIC is researching DRM deployment options that would allow DLP tools to review files before they are “wrapped” by DRM tools. This approach, in theory, would allow both tools to operate effectively. Our research is ongoing, as is the maturing of these toolsets by the commercial vendors that sell them.

We are engaging an outside firm, Booz Allen Hamilton, to review these potential solutions and provide us with an evaluation as part of an overall review of our information security and privacy program. The evaluation will inform us on any decision made on this issue.

## The SST Committee's August 1, 2016 Letter to the FDIC and the FDIC's August 25, 2016 Response

---

**Q2: The impetus for the first Science Committee hearing on FDIC data breaches was held on May 12, 2016 and looked at a series of breaches related to removable media and departing employees. What actions have the FDIC taken to prevent data breaches related to removable media and FDIC employees? Specifically, what actions have been taken since the first hearing—on May 12, 2016—and are other actions to enhance FDIC's cybersecurity procedures planned?**

**A2:** The FDIC has discontinued individuals' ability to copy information to removable media such as: external hard drives, flash drives, and CDs or DVDs, to prevent these types of incidents from occurring. Exceptions are currently limited to 2 on-site Government Accountability Office employees, 72 OIG employees, and 5 FDIC Legal Division employees (as necessary for litigation, FOIA, or Congressional requests that may necessitate removable media usage).

Additional actions to enhance FDIC's cybersecurity procedures are being implemented.

- The FDIC is revising policies and procedures such as the "Data Breach Handling Guide," and the policy circular titled "Reporting Computer Security Incidents," to better specify what actions should be taken when an incident occurs.
- The FDIC is reviewing the Data Loss Prevention tool implementation to determine how the tool can be better leveraged to safeguard sensitive information.
- The FDIC is strengthening testing of technical information security controls to confirm that the controls operate as intended.
- The FDIC is adding an information security professional position to an office that works with sensitive information.
- The FDIC will be engaging with an independent firm, Booz Allen Hamilton, to evaluate our overall information security and privacy program. That company's evaluation began August 1, 2016, and will be completed in October 2016.
- The FDIC is completing implementation of a new incident tracking system that will more centrally organize incident facts and enhance incident response management.
- The FDIC is implementing a formal insider threat program.

These are examples of a number of actions we are taking, or are planning to take, to enhance FDIC's cybersecurity program.

The FDIC's September 23, 2016 Letter to the SST Committee



FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG  
CHAIRMAN

September 23, 2016

Honorable Lamar Smith  
Chairman  
Committee on Science, Space, and Technology  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Smith:

Thank you for the opportunity to appear before the Committee at the July 14, 2016 hearing entitled *Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?* Enclosed are responses to questions asked during the hearing.

If you have additional questions, please feel free to contact me at [redacted]  
or M. Andy Jiminez, Director, Office of Legislative Affairs, at [redacted]

Sincerely,

[redacted signature block]  
Martin J. Gruenberg [redacted]

Enclosure

## The FDIC's September 23, 2016 Letter to the SST Committee

Items for Follow-up from the FDIC Chairman's July 14, 2016 Testimony to the

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY  
U.S. HOUSE OF REPRESENTATIVES

---

**Q1: Will digital rights management (DRM) implementation make the data loss prevention (DLP) tool ineffective? (Rep. Loudermilk)**

**Response:** DRM software protects information by encrypting it, by limiting how it can be used (for example whether or not it can be printed), and by limiting who has access. DLP software monitors information during a transmission process (for example, information in emails or information uploaded to a website) looking for sensitive information. Since DRM software typically encrypts information, and encrypted information cannot always be monitored by DLP software, there have been concerns raised that the implementation of DRM software will make DLP software less effective.

The FDIC is currently evaluating solutions that claim to directly integrate DLP and DRM software and researching possible FDIC integrations that could ensure DLP and DRM software function effectively, without degrading one another.

For example, makers of DLP and DRM software promote their software integration so that DLP tools can review the contents of a DRM-wrapped file. Some of these tools are not yet on the market but are promised soon. These solutions will be examined to see how effective they may be in our environment.

Separately, the FDIC is researching DRM deployment options that would allow DLP tools to review files before they are "wrapped" by DRM tools. This approach potentially would allow both tools to operate effectively. Our research is ongoing, as is the maturing of these toolsets by the commercial vendors that sell them.

We have engaged an outside firm, Booz Allen Hamilton, to review these potential solutions and provide us with an evaluation as part of an overall review of our information security and privacy program. No final decision will be made on the use of DRM software until this third-party review has been completed.

**Q2: Is classified information (generally) in the sensitive compartmented information facility (SCIF) at risk because of the use of digital rights management (DRM)? (Rep. Loudermilk)**

**Response:** The FDIC does not use DRM technology to protect classified information and thus should not put classified information in the FDIC's SCIF at risk. To the extent the FDIC works with classified information, it uses the security protections of the Intelligence Community

## The FDIC's September 23, 2016 Letter to the SST Committee

systems that are located in our SCIF. Those classified systems are not connected to the unclassified FDIC network. The agency does not own or administer the security controls of the classified information and communications systems it houses in the SCIF. The Intelligence Community controls and maintains the administrative rights for the security protocols and measures that are in place to safeguard those systems. The FDIC is only a user and consumer of those services as well as the information it retrieves from those platforms.

**Q3: Has there been a reduction in potential incidents since restricting the copying of information to removable media? (Rep. Bonamici)**

**Response:** Yes. In the first half of 2016 the FDIC implemented a prohibition on copying information to removable media. There are only 79 individuals with an authorized exception to the prohibition (72 Office of Inspector General (OIG) individuals, 5 FDIC Legal Division individuals, and 2 Government Accountability Office individuals). Latest reports show substantially reduced download activities and no breaches.

**Q4: What is the cost of switching to laptops? Won't laptops be less secure (provide a comparison of security aspects of using laptops vs remote login)? We have heard allegations that decisions are being made at the top without consulting staff, and that arbitrary deadlines have been set to complete work by July 31. Please review this and get back to us. (Rep. Neugebauer)**

**Response:** FDIC examiners and resolution specialists in the field have historically relied on laptops to carry out bank examination and resolution activity. In 2015, the FDIC replaced approximately 6,000 laptops with updated models as part of its normal technology refreshment cycle.

The FDIC began to deploy an additional 3,400 laptops to replace desktops for the workforce located principally in Washington, D.C, as well as FDIC regional offices. That deployment has been put on hold pending a third party review. The 2016 cost to deploy laptops is approximately \$1,700 per laptop, including the hardware and services.

The principal reason the FDIC began replacing desktops with laptops is that the mobility of the laptop is greater, and the security of the laptop when an individual is working outside FDIC premises would be better than other alternatives.

Mobility and security are important as the FDIC continues to improve its disaster response capability consistent with its designation as a National Security/Continuity Category II Agency. Providing a safe method for connection to the FDIC network from non-FDIC locations is critical for business continuity. FDIC-issued laptops can be a better alternative for accessing the FDIC network from outside FDIC facilities than, for example, a personally-owned device because of the FDIC's ability to better monitor and control user activity on devices it manages.

## The FDIC's September 23, 2016 Letter to the SST Committee

The FDIC employs multiple information security controls on laptops and routinely re-evaluates and improves those controls. FDIC laptop hard drives are encrypted using a commercially-available solution that is consistent with National Institute of Standards and Technology (NIST) encryption standards. Additionally, FDIC laptops are managed by information technology administrators, not the end users. End users are limited in what they are able to change on laptops because they do not have operating system administrator privileges. Laptops also have standard software configurations that are periodically updated with automated tools. Other laptop protections and controls are anti-virus, host-based intrusion prevention, data loss prevention, and application whitelisting software. The FDIC is currently deploying new mobile device management (MDM) software that could further improve laptop security controls.

There have been concerns expressed regarding the laptop security configuration and deployment timeframe. The FDIC implemented the security controls described in the previous paragraph on the 2015 laptops based on guidance from FDIC information security staff. These same controls are being used on the 2016 laptops. Although the FDIC originally set a goal of having new laptops deployed by the end of July 2016 to support improved security through the use of multi-factor authentication (Personal Identity Verification cards), we have extended that timetable to ensure security control adequacy.

The FDIC has requested a review of laptop security controls by the Booz Allen Hamilton team that was engaged in August 2016 to complete a comprehensive security assessment. No further steps will be taken until we receive the third-party review.

**Q5: What are the new laptop specifications? What is your cybersecurity budget? (Rep. Foster)**

**Response:** Below are specifications for the newest laptops, purchased in 2016, and the specifications for the approximately 6,000 laptops deployed in 2015. Security controls between the two platforms are essentially equivalent.

	<b>Newest Laptop - Dell Latitude E5470</b>	<b>2015 Laptop – Lenovo T450</b>
Processor:	6th Generation Intel Core i7-6820HQ (Quad Core, 2.7GHz, 8MB cache)	5th Generation Intel Core i7-5600U (2 Core, 2.6 GHz Base Frequency)
Operating System:	Windows 7 Professional 64 Compatible	Windows 7 Professional 64 Compatible
Display:	14" FHD (1920x1080) Anti-Glare	14" FHD (1920x1080) Anti-Glare
Graphics:	Intel HD Graphics 530	Intel HD Graphics 5500
Memory:	16GB	12GB
Keyboard:	Internal Dual Pointing Backlit (English)	Dual Pointing Backlit (English)
Hard Drive:	256GB SATA Class 10 Solid State Drive	256GB SATA3 Solid State Drive

## The FDIC's September 23, 2016 Letter to the SST Committee

System Expansion Slots:	Smart Card Reader	Smart Card Reader
Battery:	3-cell (47 Whr)	Two 3-cell Li-Polymer (23.2Whr)
Power Cord:	US Power Cord (450-AAEJ)	CPK US w/Linecord 45W AC (US 2pin)
Wireless:	Intel Dual Band Wireless 8260 with Bluetooth (555-BCMT)	Intel 11 a/g/n with Bluetooth 4.0

The information security and privacy budget is approximately \$50 million annually.

**Q6: Do you have an IT strategic plan, and will you evaluate the enterprise architecture? Provide an executive summary of the Booz Allen Hamilton engagement as well. (Rep. Bridenstine)**

**Response:** The FDIC has an IT strategic plan (enclosed) that was published on June 11, 2013, entitled, "*Business Technology Strategic Plan: 2013 – 2017.*" The plan was developed by the Division of Information Technology (DIT) in partnership with the non-IT divisions of the FDIC. The strategic plan references the enterprise architecture of the FDIC, the continuing evolution of the architecture, and our architectural principles.

One of the FDIC's 2016 performance goals is to publish, with support from The MITRE Corporation, an updated IT strategic plan by year-end. The enterprise architecture is being evaluated in concert with development of the plan and will be central to achieving IT goals.

The FDIC has engaged Booz Allen Hamilton to complete an end-to-end review of the FDIC's IT security and privacy programs to determine strengths, gaps, risks, and weaknesses in the current programs with a focus on human capital, processes, procedures, and tools. Booz Allen Hamilton began work in August 2016 and is expected to complete work in October 2016. An executive summary of that work is enclosed.

**Q7: Does the FDIC have an employee handbook? Is it clear to employees that taking sensitive information outside the agency is unacceptable? (Rep. Palmer)**

**Provide a copy of the employee handbook. (Rep. Loudermilk)**

**Response:** Rather than a single employee handbook, the FDIC, like many federal agencies, has issued a large number of internal directives to employees covering virtually all aspects of operations. These directives are available to all employees on the internal FDIC website.

These directives cover topics under the broad headings of Administration and Management, Personnel Management, Services and Facilities, Financial Management, Law and Legal Matters,



## The FDIC's September 23, 2016 Letter to the SST Committee

as well as directives related to bank supervision. One specific set of FDIC directives relates to Information Resources Management for existing employees. These directives (copies enclosed) include topics such as "Acceptable Use Policy for Information Technology Resources," "Information Technology Security Risk Management Program," "Automated Information Systems Security Program," "Protecting Sensitive Information," "Mandatory Information Security Awareness Training," "Information Technology Security Guidance for FDIC Procurements/Third Party Products," "FDIC Privacy Program," "Safeguarding FDIC Information Technology Hardware," and others. As one of the aforementioned directives indicates, the FDIC has mandatory annual information security awareness training for all managers and employees. In addition to the directives, the FDIC's Corporate University (CU), Division of Administration (DOA), and Division of Information Technology (DIT) offer programs, materials, and/or training that address information security and related areas.

Additionally, the FDIC requires departing employees and contractors to certify within the "Pre-Exit Clearance Record for Employees" (Form 2150/01, enclosed) the following:

*"All Corporation-owned property, equipment and documents that were in my possession have been returned to the proper division/office or have been accounted for ... (i) I have not removed any Confidential Information (as defined below) from FDIC premises except as necessary or appropriate in the course of my employment, disclosed any Confidential Information to any person not authorized to receive it, nor sent any Confidential Information to any address outside the FDIC (whether by mail, email or otherwise) except in accordance with applicable FDIC policies on the use and transmittal of FDIC information, and (ii) I have returned to the FDIC all Confidential Information that I possessed (in whatever form it existed) and will not transmit or remove (in any format or in any medium) any Confidential Information to any address outside the FDIC between the signing of this certification and my departure from FDIC employment.... 'Confidential Information' means... (i) of a personal nature (sometimes referred to as 'Personally Identifiable Information' or 'PII') or (ii) as it relates to certain commercial interests, to banking or financial institutions or the banking or financial industry in general, or to the overall programs and mission of the FDIC (sometimes referred to as 'Sensitive Information')... If there is a breach of this agreement, the FDIC shall be entitled to injunctive relief from such court or courts as shall have jurisdiction and such relief shall be in addition to, and not in lieu of, other remedies available to the FDIC under the law... My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (see 18 U.S.C. 1001)."*

For current employees, and as mentioned above, the FDIC's CU, DOA, and DIT offer programs, materials, and/or training that address information security and related areas. Employees must annually complete and certify understanding of the training that, in part, addresses the proper use of sensitive information.

## The FDIC's September 23, 2016 Letter to the SST Committee

**Q8: When did you learn that an FDIC lawyer had instructed staff not to discuss in writing matters related to cybersecurity and breaches? (Rep. LaHood)**

**Response:** On June 13, 2016 I received a briefing on the document production being transmitted to the Committee in response to its letter dated May 24, 2016. Among the documents I was shown included one from an FDIC lawyer that stated the following:

*"As we discussed the day before yesterday and before, I asked you not to send around your suggested ideas for interim procedures (or anyone's ideas) because there are significant questions about what should be in the procedures and we need more input before drafts are ready to circulate."*

To the best of my recollection, this is the first I was made aware of the allegation raised in the question.

**Q9: Who advised you on the insider threat program and when? Who halted the program? Explain who was involved, when, and how the decision was arrived at resulting in it stalling out. (Rep. Weber)**

**Response:** To the best of my recollection, in early April 2015, I was made aware that the FDIC's Division of Administration (DOA) was engaging in insider threat investigative activities in the absence of any FDIC insider threat policy or governance. Upon learning of DOA's activities, I requested a briefing, which was held on April 9, 2015 and included the following individuals: Arleas Upton Kea, Director, DOA; Ron Bell, Deputy Director, DOA; Christopher Farrow, CISO; Roberta McInerney, Deputy General Counsel; [REDACTED]; and Barbara Ryan, Deputy to the Chairman and Chief Operating Officer/Chief of Staff (COO/COS). That briefing was followed by a second briefing with the same attendees and Charles Yi, General Counsel, on April 10, 2015. At the briefings I was informed about the development of the program and its activities to date. Concerns were raised during the meeting regarding employee privacy rights and the need for a careful, deliberative approach. At the April 10, 2015 briefing, I asked that a governance framework and appropriate policies, procedures, and controls be developed by DOA, together with the Legal Division and the Office of the Chief Information Officer, to ensure that the program was conducted in a manner consistent with the FDIC's authorities.

Following the two April 2015 briefings, the COO/COS requested that DOA bring the draft policies and procedures to senior management for review when complete. In the interim, the topic was added to an ongoing list of operational topics for future discussion by senior management. On July 24, 2015 DOA reported to the FDIC Intelligence and Critical Infrastructure Protection Committee, a senior level interdivisional committee focused on information technology and cybersecurity issues, that a governance framework/policy and procedures draft directive for the program had been developed and that DOA would vet a final draft with other divisions in September 2015. As discussed below, this did not come to completion in a timely manner. DOA next briefed senior management in March 2016 to provide another update on the ongoing development of the program.

## The FDIC's September 23, 2016 Letter to the SST Committee

I am not aware that the program was halted. The focus of the activities shifted to the development of policies and procedures. I understand that DOA's Counterintelligence Officer, who had responsibility for the development of the program, resigned in the fall of 2015 and the position was not filled. It is also my understanding that competing priorities within DOA may have affected the timing of the development of the program during this period. DOA also was rolling out an Active Shooter Program in all regions of the agency and playing a key role in the deployment of Personal Identity Verification (PIV) cards to all employees and contractors. Several of the individuals responsible for the development of the Insider Threat and Counterintelligence Program (ITCIP) policies and procedures also were responsible for the completion of these projects.

This governance framework, with appropriate policies and procedures, has now been finalized and has received appropriate reviews and approvals. I formally approved the ITCIP on Wednesday, September 21, 2016 and the program policies and procedures were posted to an internal website and communicated to all employees on September 22, 2016.

The FDIC's Office of the Inspector General is currently reviewing this matter and will report separately to Congress.

**Q10: Why was there five weeks of delay between a March incident and the May reporting of it? (Rep. Beyer)**

**Response:** The FDIC received an OIG memorandum regarding congressional notification of the Florida Incident on February 19, 2016, while the OIG's audit was still ongoing. The FDIC then proceeded to give Congress notification of the Florida Incident on February 26, 2016. In light of the OIG's recommendations, the FDIC also conducted a retrospective review of other incidents that had occurred since issuance of OMB Guidance M-16-03.

Once the retrospective review was completed, five incidents were reported to Congress on May 9, 2016, and to the OIG. One of the five major incidents identified in the retrospective review was an incident discovered on December 10, 2015 and determined to be major by a Data Breach Management Team on March 28, 2016 as part of the retrospective review. The results of all the incidents determined to be major during the retrospective review were compiled in the May 9, 2016 report to Congress.

The FDIC processes have since been improved so that major incident reporting is within seven days after the date on which there is a reasonable basis to conclude that a major incident has occurred.

## The SST Committee's May 10, 2016 Letter to the OIG and the OIG's May 11, 2016 Response

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 10, 2016

Mr. Fred W. Gibson  
Acting Inspector General  
Federal Deposit Insurance Corporation  
3501 Fairfax Drive  
Arlington, VA 22226

Dear Mr. Gibson,

The Committee on Science, Space, and Technology is continuing its oversight of recent cybersecurity events at the Federal Deposit Insurance Corporation (FDIC). As you know, the Committee wrote to the FDIC on April 8, 2016 and April 20, 2016 about two separate cybersecurity breaches.<sup>1</sup> The Committee's April 20, 2016 letter concerned an October 2015 cybersecurity breach, involving an FDIC employee who copied personal information and customer data for over 10,000 individuals onto a portable storage device prior to separating from agency employment.<sup>2</sup> Most troublesome, the FDIC withheld information from Congress about the incident for over four months until urged to report the incident to Congress by your office in accordance with the Federal Information Security Modernization Act of 2014 and Office of Management and Budget guidelines.<sup>3</sup> Although the FDIC responded to the Committee's letter and certified that it produced all responsive documents to the Committee,<sup>4</sup> subsequent discussions with your office indicate that the Office of Inspector General (OIG) has responsive documents that were apparently withheld by the agency. We request that your office produce, to the best of your knowledge, any responsive documents that remain outstanding.

<sup>1</sup> 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]; 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].

<sup>2</sup> Letter, Apr. 20, 2016, *supra* note 1.

<sup>3</sup> *Id.*; 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 10, 2016).

<sup>4</sup> Phone Call with H. Comm. on Science, Space, & Tech. Staff & Fed. Deposit Insurance Corp. Staff (May 6, 2016).

## The SST Committee's May 10, 2016 Letter to the OIG and the OIG's May 11, 2016 Response

Mr. Fred W. Gibson  
May 10, 2016  
Page 2

Given that the FDIC has recently experienced two significant security breaches, which compromised, in aggregate, over 54,000 customers' sensitive data,<sup>5</sup> the Committee is increasingly concerned about the FDIC's overall cybersecurity posture. Further, because of the FDIC's apparent hesitation to report the October 2015 incident to Congress, the Committee has held long-standing concerns about the agency's willingness to be forthcoming and transparent with Congress. The revelation that the agency chose to withhold responsive documents from the Committee, despite agency staff certifying that all responsive materials have been produced, compounds the Committee's concerns about the agency's openness with Congress. Specifically, FDIC's decision to withhold responsive materials raises serious questions about agency's veracity when communicating with congressional staff regarding the completeness of the agency's production. The Committee is concerned that by attempting to shield information from Congress, the FDIC is endeavoring to skirt congressional oversight and avoid answering serious questions about the agency's cybersecurity posture. Withholding information from Congress is unlawful under Title 18 of the U.S. Code.<sup>6</sup> We will be investigating FDIC's failure to produce all responsive documents with this statute in mind.

During discussions with your office concerning the outstanding documents, your staff conveyed to Committee staff your office's approach of allowing the agency to produce its own internal documents in response to congressional requests. While the Committee understands the OIG's approach to allow the agency to produce documents that were created by the agency and are in the agency's possession, the Committee understands that the withheld documents are directly responsive to the Committee's outstanding request. Further, given that the outstanding documents are responsive to the Committee's request, these documents are essential to furthering the Committee's understanding of the agency's approach to responding to security breaches. To assist in the Committee's ongoing oversight of the FDIC's responses to the recent security incidents, please provide all of the responsive materials in unredacted format in your office's possession that remain outstanding.

The Committee on Science, Space, and Technology has jurisdiction over environmental and scientific programs and "shall review and study on a continuing basis laws, programs, and Government activities" as set forth in House Rule X.

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

<sup>5</sup> See Letter, Apr. 8, 2016, *supra* note 1; Letter, Apr. 20, 2016, *supra* note 1.

<sup>6</sup> Title 18 U.S.C. 1505, reads in pertinent part:

Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress—

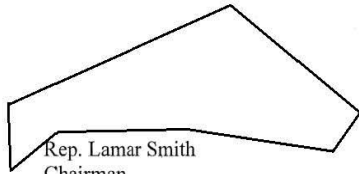
Shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.

The SST Committee's May 10, 2016 Letter to the OIG and the OIG's  
May 11, 2016 Response

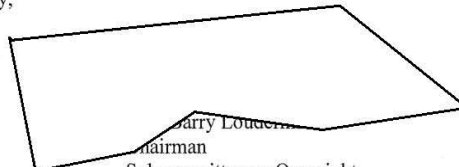
Mr. Fred W. Gibson  
May 10, 2016  
Page 3

Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact [redacted] or [redacted]  
[redacted] at [redacted]. Thank you for your attention to this matter.

  
Rep. Lamar Smith  
Chairman  
Committee on Science, Space, and Technology

Sincerely,

  
Harry Loudermilk  
Chairman  
Subcommittee on Oversight

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

The SST Committee's May 10, 2016 Letter to the OIG and the OIG's  
May 11, 2016 Response



Federal Deposit Insurance Corporation

3501 Fairfax Drive, Arlington, Virginia 22226

Office of Inspector General

TRANSMITTED VIA ELECTRONIC MAIL

May 11, 2016

Honorable Lamar Smith  
Chairman  
Committee on Science, Space, and Technology  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Smith:

I am writing in response to your letter, dated May 10, 2016, requesting that our office produce certain Federal Deposit Insurance Corporation (FDIC) documents. As you note in your letter, it is not our office's practice to produce FDIC documents. However, based on your specific request that we do so in this instance, we are producing FDIC documents in our possession that the Corporation has provided to us during the course of our audit entitled *The FDIC's Process for Identifying and Reporting of Major Security Incidents*.

Our office is not in the position to assert nor waive privileges that the FDIC might assert over its documents. Nonetheless, many of the enclosed documents contain highly sensitive and private information. Specifically, these documents include FDIC employee names; internal FDIC supervisory guidance; FDIC attorney communications, analyses, meeting notes, and emails; and references to open banks and bank customers. These documents are not publicly available and are not intended for public release. We ask that you safeguard the contents of all enclosed documents. Additionally, we do not consider providing you with the enclosed information to be a waiver of any applicable privileges or a public release under the Freedom of Information Act.

While your letter requested that we provide these documents in their unredacted form, we have made some limited redactions that were agreed to by your staff. We do not believe such redactions will impede your understanding of the documents.

If you have any questions, please feel free to contact me at [redacted] or [redacted].  
[redacted] of my staff is also available to assist you and can be reached at [redacted] or [redacted].

Sincerely,

[redacted signature block]

Fred W. Gibson, Jr.  
Acting Inspector General

Enclosure

cc: Honorable Eddie Bernice Johnson, Ranking Member

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

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 24, 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 recent security events at the Federal Deposit Insurance Corporation (FDIC).<sup>1</sup> Following the Committee's May 12, 2016 hearing, during which representatives from the FDIC testified,<sup>2</sup> additional information has come to light regarding the effectiveness of the agency's cybersecurity measures, attempts to circumvent providing full and complete responses to the Committee's requests, and concerns that the agency may attempt to take retaliatory action against whistleblowers. Because of this new information, the Committee is writing to request additional documents and transcribed interviews with key individuals who have played a role in managing the agency's cybersecurity initiatives, as well as individuals who have been involved with the agency's production of requested materials to the Committee.

In recent weeks, the Committee has learned additional information about significant shortfalls in the agency's cybersecurity practices intended to guard against data security breaches. Although the FDIC's Chief Information Officer and Chief Privacy Officer, Lawrence Gross, testified at the hearing that the "FDIC has a strong information security program to identify events that could signal a data security incident,"<sup>3</sup> the Committee has obtained information in contradiction of this statement. Mr. Gross' testimony was a misrepresentation, at best, of the strength of the agency's cybersecurity posture.

While all of the cybersecurity incidents reported to Congress in the last three months have involved departing employees, Mr. Gross represented during the hearing that this fact was simply a coincidence.<sup>4</sup> In reality, however, the FDIC apparently has not focused its

<sup>1</sup> 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).

<sup>2</sup> H. Comm. on Science, Space, & Tech., *FDIC Data Breaches: Can Americans Trust that Their Private Banking Information is Secure?*, 114<sup>th</sup> Cong. (May 12, 2016) [hereinafter FDIC Hearing, May 12, 2016].

<sup>3</sup> See Statement of Lawrence Gross, Chief Information Officer, Fed. Deposit Insurance Corp. (May 12, 2016), at 5 (emphasis added).

<sup>4</sup> FDIC Hearing, May 12, 2016, *supra* note 2, at 40, 58.



## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

The Honorable Martin J. Gruenberg  
May 24, 2016  
Page 2

cybersecurity efforts on monitoring current employees' computer activity, including whether current employees are downloading sensitive information on to portable storage devices. Although the FDIC monitors departing employees' computer activity, it has apparently opted to forego taking a close look at the computer activity of individuals who remain employed at the agency. This leaves important information, including personally identifiable banking information for millions of Americans and banks' living wills, vulnerable to data breaches by FDIC employees, who currently have access to sensitive information at the agency.

Additionally, while the Committee applauds the success of the FDIC's Data Loss Prevention (DLP) program, which was responsible for catching each of the recent data breaches involving a departing employee, the Committee has since learned that the same program is *incapable* of detecting if an employee copies, downloads, or otherwise transfers encrypted information from FDIC systems. This information raises serious concerns about whether additional data breaches have occurred without detection due to inherent weaknesses in the FDIC's systems used to monitor data breaches. Even more troublesome, the Committee is concerned that Mr. Gross was not forthcoming during his recent testimony about significant information regarding vulnerabilities within the agency's cybersecurity programs.<sup>5</sup>

Regrettably, the FDIC's decision to withhold information pertinent to its cybersecurity posture is yet another example of the agency's continued reticence to being fully transparent with the Committee's investigation. According to information obtained by the Committee, FDIC officials charged with identifying and producing responsive documents to the Committee's requests regarding the recent data breaches have actively worked to limit the scope of the Committee's requests such that the universe of responsive information falls far short of a full and complete production to the Committee. In fact, during the hearing, Members of the Committee questioned Mr. Gross about whether anyone at the agency voiced any concern regarding the manner, scope, or methods the agency employed to identify and gather responsive documents.<sup>6</sup> Although Mr. Gross both denied that the agency limited the scope of the Committee's requests or that anyone at the agency voiced any concerns,<sup>7</sup> information obtained by the Committee raises questions about the veracity of Mr. Gross' testimony. So that the Committee can determine whether the FDIC improperly limited the scope of the Committee's requests and whether anyone at the agency raised concerns about how the FDIC determined the scope of the Committee's requests, please produce all documents and communications referring or relating to these matters.

As Committee Members explained during the hearing, the FDIC has repeatedly attempted to shield information from Congress. When providing responses to the Committees' letters, the FDIC initially produced documents redacted extensively for information the agency deemed to be "confidential." Despite the agency's inability to cite statutory authority or a valid privilege for redacting information, the agency resisted the Committee's request for providing unredacted documents until faced with the threat of the Committee's use of the compulsory process to obtain

<sup>5</sup> Letter from Hon. Lamar Smith, Chairman, H. Comm. on Science, Space, & Tech., to Hon. Martin Gruenberg, Chairman, Fed. Deposit Insurance Corp. (May 19, 2016).

<sup>6</sup> FDIC Hearing, May 12, 2016, *supra* note 2, at 28–29.

<sup>7</sup> *Id.*

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

The Honorable Martin J. Gruenberg  
May 24, 2016  
Page 3

unredacted documents. These redactions included the name of the employee responsible for the October 2015 security breach in Florida. Ironically, this employee was the same individual the Committee found, in fact, to have received a Master of Information Technology Management, despite Mr. Gross' testimony that she was not proficient with using computers.<sup>8</sup> As an agency that has faced a seemingly never ending series of security breaches, it should focus its resources first and foremost on reforming its internal cybersecurity mechanisms, instead of endeavoring to conceal information from the Committee.

Additionally, according to information obtained by the Committee, agency personnel have reportedly instructed FDIC employees to avoid placing things in writing, including information related to the agency's data breaches. If true, these allegations raise serious concerns about whether the agency is attempting to circumvent federal records requirements, diminish the universe of information that could be responsive to congressional requests, and ultimately hide the truth from congressional overseers.

In light of the serious nature of these allegations, I request that all documents responsive or related to the Committee's requests and communications between and among employees of the FDIC referring or relating to the Committee's requests, be preserved. So that a full and complete record of documents may be provided to the Committee in response to future document requests that the Committee may deem appropriate, please:

1. Preserve all e-mail, electronic documents, handwritten documents, and data created since January 1, 2009, concerning the FDIC's cybersecurity posture, including any and all information related to data breaches.

For the purpose of this request, "preserve" means taking reasonable steps to prevent the partial or full destruction, alteration, testing, deletion, shredding, incineration, wiping, relocation, migration, theft, or mutation of electronic records, as well as negligent or intentional handling that would make such records incomplete or inaccessible.

2. Exercise reasonable efforts to identify and notify former government employees, and any other relevant third party who may have access to such electronic records, that they are to be preserved; and,
3. If it is a routine practice of any agency employee, contractor, or related third party to destroy or otherwise alter such electronic records, either halt such practices or arrange for the preservation of complete and accurate duplicates or copies of such records, suitable for production if requested.

To assist the Committee in answering outstanding questions material to its ongoing investigation, we request that you make the following individuals, listed in no particular order, available for a transcribed interview by Committee staff:

---

<sup>8</sup> *Id.* at 40.

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

The Honorable Martin J. Gruenberg  
May 24, 2016  
Page 4

1. Roberta K. McInerney, Deputy General Counsel (Consumer and Legislation)
2. Andy Jiminez, Director, Office of Legislative Affairs
3. Christopher J. Farrow, Special Advisor
4. [REDACTED] Special Assistant, Information Security and Privacy Staff
5. [REDACTED] Acting Chief Information Security Officer, Information Security and Privacy Staff
6. [REDACTED] Deputy Director, Infrastructure Services Branch
7. [REDACTED] Incident Lead
8. [REDACTED] Information Technology Specialist
9. Henry Griffin, Assistant General Counsel

Please contact Committee staff by May 31, 2016, to schedule the requested interviews. Additionally, please provide all documents and communications referring or relating to FDIC's response(s) to my letters dated April 8 and 20, 2016, including but not limited to documents showing that employees raised concerns related to the scope of the Committee's requests and how the FDIC determined the scope of the Committee's requests, by June 7, 2016. Further, the Committee anticipates holding an additional hearing on the FDIC's cybersecurity posture. Please ensure you are available to testify at a hearing on July 14, 2016.

Finally, as the Committee continues its investigation, we would like to remind you of the protections for whistleblowers found in the Whistleblower Protection Act (WPA).<sup>9</sup> As you should know, the WPA is a key tool for rooting out wrongdoing and serves as the foundation for delineating rights of whistleblowers. Often, whistleblowers function as the primary means for informing Members of Congress of misconduct within the Executive Branch. Any action taken against whistleblowers not only has a chilling effect on the willingness of federal employees to report waste, fraud, and abuse, but is unlawful. The Committee takes seriously any concerns regarding reprisal against whistleblowers and will investigate accordingly, if allegations are brought to the Committee's attention.

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.

<sup>9</sup> 5 U.S.C. § 7211 provides in pertinent part: "The right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied."

**The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's  
June 7, 2016 Response**

The Honorable Martin J. Gruenberg  
May 24, 2016  
Page 5

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 [redacted] or [redacted] at [redacted]. Thank you for your attention to this matter.

Sincerely,

[redacted]

Lamar Smith  
Chairman

[redacted]

Loudermilk  
Chairman  
Subcommittee on Oversight

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

Enclosure

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

---

### 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.

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

---

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

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

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.

**The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's  
June 7, 2016 Response**

---

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.



The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's  
June 7, 2016 Response



Federal Deposit Insurance Corporation  
550 17th Street NW, Washington, DC 20429

June 7, 2016

Honorable Lamar Smith  
Chairman  
Committee on Science, Space, & Technology  
House of Representatives  
Washington, D.C. 20515

Honorable Barry Loudermilk  
Chairman  
Subcommittee on Oversight  
House of Representatives  
Washington, D.C. 20515

Dear Chairman Smith and Chairman Loudermilk:

I am writing in response to your letter of May 24, 2016, requesting additional documents regarding Federal Deposit Insurance Corporation cybersecurity posture as well as interviews with certain identified individuals.

A DVD containing additional documents responsive to your earlier requests and a description of the search parameters used to identify the documents requested is enclosed with this response. As discussed in further detail in the enclosure, the FDIC is continuing to review documents from the results of the search and will provide responsive materials on a rolling basis. In addition, the FDIC has already arranged with your staff interviews with each of the individuals identified in the request.

If you or Committee staff have any questions, please contact

[Redacted]

[Redacted]

Sincerely,

[Redacted Signature]

Charles Yi  
General Counsel

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

Enclosure: DVD  
Document Request Response

## The SST Committee's May 24, 2016 Letter to the FDIC and the FDIC's June 7, 2016 Response

### Document Request Response

The enclosed DVD contains a partial production of additional documents that have been identified as responsive to the Committee's document requests dated April 8, 2016 and April 20, 2016. As discussed with your staff, these documents were identified by an electronic search of the FDIC's e-mail database for the following terms: "Florida incident," "M-16-03," as well as CSIRT Incident numbers "224983" and "221387." Documents identified by this search and determined to be responsive to the matters discussed in the Committee's requests have been provided on the enclosed DVD. As discussed with your staff, the FDIC is continuing to review documents from the results of this search and will provide responsive documents on a rolling basis.

As also discussed with your staff, the FDIC continues to conduct additional searches in response to the Committee's May 24, 2016 letter. We have initiated a search in the FDIC's e-mail database for documents of individuals we believe to be responsive that contain the terms "committee," "concern," "congressional," "Hill," "letter," "limit," "request," "response," "science," "scope," or "Smith." Should the documents identified by these searches prove overly voluminous, we will continue to work with your staff to develop effective search parameters and will produce responsive documents as they are available.

The Bates range for the documents on the enclosed DVD is FDICSSTIV0000001 – FDICSSTIV0001408. The enclosed DVD has been encrypted. The password for the DVD will be transmitted to your staff by separate email. If necessary, the FDIC can provide a technical specialist to assist the Committee with accessing the documents.

Please be advised that some of the documents produced today may contain personally identifiable information, sensitive, confidential, and/or proprietary information about financial institutions.

For documents that the FDIC is providing to the Committee, the FDIC has clearly marked those documents that it considers privileged or confidential. The FDIC does not believe that this or any future production of documents to the Committee affects a waiver of any privileges that may apply. For example, some of the documents may have been generated in connection with the FDIC's decision-making process and are thus protected by the deliberative process privilege. Some documents may contain confidential attorney-client communications protected by the attorney-client privilege. Moreover, apart from privileges applicable to the FDIC, some of the documents produced today may include privileged information belonging to third-parties including financial institutions. Production by the FDIC of any such third-party information should not be construed as a waiver of any applicable privileges. The FDIC respectfully requests that the Committee respect all applicable privileges and the confidentiality of the information contained in the documents.

In addition, the FDIC respectfully requests that the Committee give prior notice to the FDIC of any proposed release by the Committee of any non-public information contained in any of the documents that the FDIC is providing pursuant to the Committee's request. Due to the highly confidential nature of some of the information being provided, the FDIC requests that at the conclusion of its investigation, the Committee dispose of the documents in a manner that preserves their confidentiality or return the documents to the FDIC.

## Glossary of Terms

Term	Definition
Advanced Persistent Threat (“APT”)	An APT is a network attack in which a cyber criminal or threat actor uses multiple phases to break into a network, avoid detection, and harvest valuable information over a long period of time.
Breach	OMB defines the term breach as a type of security incident that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. A breach can be inadvertent, such as a loss of hard copy documents or portable electronic storage media, or deliberate, such as a successful cyber-based attack by a hacker, criminal, or other adversary.
Data Loss Prevention (“DLP”) Tool	The DLP tool is software that is designed to detect and, if enabled, prevent potential data breaches by monitoring, detecting, and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
Digital Rights Management (“DRM”)	Digital rights management is a systematic approach to protection of digital information to prevent unauthorized redistribution of the information.
Flash Drive	A flash drive is a small electronic device containing flash memory that is used for storing data or transferring it to or from a computer, digital camera, etc.
Incident	An incident is an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information Security Manager (“ISM”)	ISMs are located within FDIC divisions and offices and provide a business focus on information security and coordinate with the CIO Organization to ensure that security controls are in place to protect their respective division or office’s information and systems. ISMs are responsible for such things as educating employees and contractors on how to properly safeguard FDIC information, ensuring that security requirements are addressed in new and enhanced systems, and promoting compliance with security policies and procedures.

## Glossary of Terms

---

Term	Definition
Major Incident	<p>According to OMB Memorandum M-16-03, a “major incident” will be characterized by a combination of the following factors:</p> <ul style="list-style-type: none"> <li>(1) involves information that is Classified, Controlled Unclassified Information (“CUI”) proprietary, CUI Privacy, or CUI Other; and</li> <li>(2) is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and</li> <li>(3) has a high or medium functional impact to the mission of an agency; or</li> <li>(4) involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either: (a) a specific threshold of number of records or users affected; or (b) any record of special importance.</li> </ul>
Personally Identifiable Information (“PII”)	<p>FDIC Circular 1360.9, <i>Protecting Sensitive Information</i>, defines PII as any information about an individual maintained by the FDIC that can be used to distinguish or trace that individual’s identity, such as their full name, home address, email address (non-work), telephone numbers (non-work), Social Security Number, driver’s license/state identification number, employee identification number, date and place of birth, mother’s maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, personal identification number), medical information, investigation report or database, criminal or employment history or information, or any other personal information that is linked or linkable to an individual.</p>
Resolution Plans	<p>Section 165(d) of the Dodd-Frank Act requires each bank holding company with total consolidated assets of \$50 billion or more and each nonbank financial company designated by the Financial Stability Oversight Council</p>

## Glossary of Terms

---

Term	Definition
	<p>(“FSOC”) for enhanced supervision by the Federal Reserve Board (“FRB”) to report periodically to the FDIC, FRB, and FSOC on the plan of such company for its rapid and orderly resolution in the event of material financial distress or failure – its resolution plan. These resolution plans are also known as “living wills.” To implement this requirement, the FDIC and FRB jointly issued a Final Rule, entitled <i>Resolution Plans Required</i>, on November 1, 2011, that requires financial companies covered by the statute to submit resolution plans describing the company’s strategy for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure of the company.</p>
Sensitive Information	<p>In general, sensitive information is information that contains an element of confidentiality. It includes information that is exempt from disclosure by the Freedom of Information Act (5 U.S.C. § 552) and information whose disclosure is governed by the Privacy Act of 1974 (5 U.S.C. § 552a). Sensitive information requires a high level of protection from loss, misuse, and unauthorized access or modification.</p>
Systemically Important Financial Institution (“SIFI”)	<p>The term SIFI refers to bank holding companies with \$50 billion or more in total consolidated assets and nonbank financial companies designated by the FSOC for FRB supervision and the enhanced prudential standards of the Dodd-Frank Act (12 U.S.C. §§ 5322 and 5323).</p>
United States Computer Emergency Readiness Team (“US-CERT”)	<p>Established in 2003, the US-CERT’s mission is to protect the nation’s internet infrastructure. US-CERT coordinates defense against and responses to cyber-attacks across the nation. In the event of a loss or compromise of business sensitive information and/or PII, US-CERT is responsible for notifying appropriate officials in the executive branch of the government about the breach incident; coordinating communications of the breach incident with other agencies; and for PII incidents, distributing to designated officials in the agencies and elsewhere a monthly report</p>

## Glossary of Terms

---

Term	Definition
	identifying the number of confirmed breaches of PII and making available a public version of the report.
Universal Serial Bus (“USB”)	USB is the most common type of computer port used in today's computers and can be used to connect keyboards, printers, removable media drives, etc. to a computer.

## Acronyms and Abbreviations

Acronym/Abbreviation	Explanation
AGC	Assistant General Counsel
APT	Advanced Persistent Threat
BSA	Bank Secrecy Act
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPO	Chief Privacy Officer
CSIRT	Computer Security Incident Response Team
CTR	Currency Transaction Report
CUI	Controlled Unclassified Information
DBHG	Data Breach Handling Guide
DBMT	Data Breach Management Team
DCP	Division of Depositor and Consumer Protection
DGC	Deputy General Counsel
DIT	Division of Information Technology
DLP	Data Loss Prevention
Dodd-Frank Act	Dodd–Frank Wall Street Reform and Consumer Protection Act
DRR	Division of Resolutions and Receiverships
GAO	Government Accountability Office
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act of 2002
FISMA 2014	Federal Information Security Modernization Act of 2014
FRB	Federal Reserve Board
FSOC	Financial Stability Oversight Council
FTC	Federal Trade Commission
ICAM	Identity, Credential, and Access Management
IRA	Incident Risk Analysis form
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
NIST	National Institute of Standards and Technology
OCFI	Office of Complex Financial Institutions
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OMB	Office of Management and Budget
ORE	Owned Real Estate
PCM	Privacy Continuous Monitoring

## Acronyms and Abbreviations

---

<b>Acronym/Abbreviation</b>	<b>Explanation</b>
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PRA	Paperwork Reduction Act
QFR	Questions-for-the-Record
RMS	Division of Risk Management Supervision
SAOP	Senior Agency Official for Privacy
SAR	Suspicious Activity Report
SIFI	Systemically Important Financial Institution
SP	Special Publication
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
U.S.C.	United States Code



## The FDIC's Response to This Report



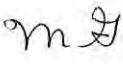
**Federal Deposit Insurance Corporation**

3501 Fairfax Drive, Arlington, VA 22226-3500

Office of the Chairman

**DATE:** March 26, 2018

**TO:** Stephen M. Beard  
Deputy Inspector General for  
Strategy and Performance

**FROM:** Martin J. Gruenberg   
Chairman

**SUBJECT:** Management Response to the OIG's Draft Special Inquiry Report Entitled *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (March 2018)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft special inquiry report entitled *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches*, dated March 12, 2018. We appreciate the OIG's special inquiry and the opportunity to provide this response. Preventing and properly responding to data breaches; strengthening our cybersecurity program; as well as providing timely, full, and accurate responses to Congressional requests are among FDIC's highest priorities. In that regard, the FDIC has implemented a number of improvements to address the matters discussed in the OIG's report. These matters will continue to receive our full attention and resources.

Over the past year, the FDIC has made progress in strengthening the agency's security posture and Breach Response Program. For example, the FDIC expanded and enhanced its Breach Response Program by elevating the agency's Chief Information Security Officer (CISO) position to the Office of Chief Information Security Officer (OCISO) which now has a dual-reporting relationship to the FDIC Chairman and to the Chief Information Officer (CIO). We also created a new Privacy Section under the OCISO which includes a new Section Chief and several key personnel. These new organizational changes along with the recent addition of an Incident Coordinator and Information Security Manager within the OCISO underscore the FDIC's commitment to improving the agency's cybersecurity and data breach management functions.

In addition, the FDIC updated its Breach Response Plan (BRP) to align with the Office of Management and Budget (OMB) M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), and to establish a consistent, repeatable process for assigning impact levels of breaches based on the risk of harm to individuals. The revised BRP outlines the procedures for managing breaches of personally identifiable information and specifies the roles and responsibilities of all FDIC personnel with access to FDIC information and systems, including the requirement to immediately report all breaches to

## The FDIC's Response to This Report

the FDIC. The BRP also defines the breach response metrics to be tracked and reported in accordance with OMB M-17-12.

Under the revised BRP, the FDIC held its first annual breach response tabletop exercise, in December 2017. The tabletop exercise was a successful first step in testing the FDIC's revised policies and procedures for managing a breach. The results of that exercise are currently being reviewed for possible future improvements in the BRP. Additionally, the FDIC completed targeted training for Breach Response Team members and consultative officials that highlighted the separate processes for, notifying individuals who have been impacted by a breach and offering credit monitoring services to such individuals.

FDIC staff has also taken steps over the past year to improve adherence to existing procedures for departing employees and contractor employees. In particular, we have improved the forms that must be signed by departing employees (with similar enhancements being integrated into the process for departing contractor employees) to incorporate a certification that the departing individual is not taking FDIC information and has returned all FDIC information and equipment.

With regard to policies and procedures relating to legal holds, the Legal Division recently implemented a new Legal Hold System that will improve the issuance and tracking of legal holds and is in the process of revisiting and, where necessary, revising its legal hold policies and procedures as they appear in related directives and guidelines. These various steps will further ensure that relevant personnel and sources of documents and information will be included in the scope of future legal holds.

We believe that corrective actions already taken and actions currently underway in response to the OIG's special inquiry report will further improve and strengthen the FDIC's breach response process. The OIG made 13 recommendations in your report. We concur with all 13 recommendations and have outlined below our planned corrective actions and estimated completion dates for each. The FDIC will carefully assess the performance issues mentioned in the special inquiry report and advise the OIG regarding decisions made to address these issues.

## The FDIC's Response to This Report

### MANAGEMENT RESPONSE

We recommend that the FDIC:

1. Ensure that revised incident and breach response guidance clearly defines the roles and responsibilities for each participant in the incident response lifecycle, including the DBMT members, Chief Information Security Officer, Chief Information Officer, Chief Privacy Officer/Senior Agency Official for Privacy, Chief Operating Officer, and Chairman and the participants are advised of and trained in those roles.

**Management Decision: Concur**

**Corrective Action:**

The CIOO completed a comprehensive update of the FDIC Breach Response Plan in October 2017, which included but was not limited to clarifying the roles and responsibilities of the CISO, CIO, Chief Privacy Officer/Senior Agency Official for Privacy (CPO/SAOP), and the Chairman. The CIOO will further update the Breach Response Plan to include the roles and responsibilities of FDIC's Chief Operating Officer as part of the incident response lifecycle.

As per OMB M-17-12, the Chairman appointed members of the Breach Response Team and delegated in writing that the CIO/CPO is the designated signatory on notification letters sent to individuals affected by a breach. Additionally, the Breach Response Plan outlines that the Chairman is the final authority for designating a breach as a Major Incident in consultation with the CPO/SAOP and CISO, and based upon the recommendation of the Breach Response Team.

Further, the CIOO provided training to Breach Response Team members in Q4 2017 to ensure they understood their respective roles and responsibilities at each stage of the FDIC's breach response lifecycle. Additionally, in December 2017, the CIOO conducted a tabletop exercise to reinforce training and identify areas for improvement. This process will be repeated at least annually to ensure members keep their knowledge updated and that the Breach Response Plan is kept current.

**Estimated Completion Date:** June 30, 2018

2. Establish procedures for identifying, tracking, and providing guidance on the applicability and implementation of new statutory requirements and government-wide guidance.

**Management Decision: Concur**

## The FDIC's Response to This Report

**Corrective Action:**

The CIOO's Audit and Internal Controls Section (AICS) has been tracking updates to OMB guidance and assigning any needed follow-up work to the appropriate managers within the CIOO, and will follow a similar process for Executive Orders, Binding Operational Directives and privacy guidance. In connection with the various actions described above, the CIOO and AICS will continue to coordinate with the Legal Division (and other divisions or offices as appropriate) to the extent necessary in determining appropriate responses to new statutory requirements and government-wide guidance. The CIOO will document the procedures for identifying, tracking, and providing guidance on the applicability and implementation of new statutory requirements and government-wide guidance.

**Estimated Completion Date:** June 15, 2018

3. Establish procedures that describe the manner in which legal opinions are developed, deliberated, and provided to divisions and offices and that are consistent with legal, regulatory, and/or operational requirements for records management.

**Management Decision:** Concur

**Corrective Action:**

The Legal Division will establish procedures by which legal opinions are developed, deliberated, disseminated, and maintained. Such procedures will include the manner in which legal opinions are to be shared with divisions and offices that are stakeholders with respect to the subject matter in question, e.g., data breach management and related topics, and such opinions shall be consistent with legal, regulatory, and/or operational requirements for records management.

**Estimated Completion Date:** July 30, 2018

4. Emphasize that consumer notification of a breach should be considered separate from the decision to offer credit monitoring services.

**Management Decision:** Concur

**Corrective Action:**

The CIOO completed an update of the FDIC Breach Response Plan in October 2017. This update included distinct decision paths for consumer notification and credit monitoring. In November and December 2017, the CIOO provided training

## The FDIC's Response to This Report

to the BRT members that addressed (among other things) the distinct decision paths for consumer notification and credit monitoring.

**Estimated Completion Date:** Completed -- December 31, 2017

5. Establish responsibility and adhere to established timeframes for reporting incidents to FinCEN where SAR information has been compromised.

**Management Decision:** Concur

**Corrective Action:**

The Division of Risk Management Supervision (RMS) issued Regional Director (RD) memorandum, *Protecting Bank Secrecy Act Information and Maintaining the Confidentiality of Suspicious Activity Reports* ("guidance") on December 27, 2016. This guidance incorporates the *Bank Secrecy Act Information Access Security Plan* ("Security Plan") with which each authorized user of the Financial Crimes Enforcement Network ("FinCEN") database must comply. The Security Plan implemented the requirement to immediately notify FinCEN concerning any apparent, threatened or possible BSA data compromise or loss.

RMS has shared this information with examiners and other RMS staff in the form of an official RD memorandum and through multiple conference calls. RMS will continue to provide reminders to all staff annually that information maintained in, or available through, the FinCEN database is sensitive – and in some instances confidential – and may only be retrieved and used for official FDIC business.

RMS will continue to coordinate with the CIOO and the Legal Division as appropriate, particularly with respect to the responsibility and timeframes for reporting incidents to FinCEN where SAR information has been compromised. In addition, in May 2018, RMS will issue a global email reminder regarding the requirement to report incidents to FinCEN when SAR information has been compromised.

**Estimated Completion Date:** June 30, 2018

6. Ensure that all key officials involved in incident responses are required to participate in periodic tabletop exercises to test the incident response plan.

**Management Decision:** Concur

## The FDIC's Response to This Report

### **Corrective Action:**

The FDIC Breach Response Plan, updated in October 2017, requires that an annual breach response tabletop exercise be performed. Pursuant to the Breach Response Plan, the key members of the Breach Response Team (BRT) are required to participate in the breach response tabletop exercise. In December 2017, a breach response tabletop exercise was completed to test the new plan and ensure that members of the BRT were familiar with the plan and understand their specific roles. Furthermore, as provided in the Breach Response Plan, those key officials designated as members of the BRT will continue to participate in future breach response tabletop exercises.

**Estimated Completion Date:** Completed – first tabletop held December 13, 2017.

7. Ensure that annual reviews established in the Breach Response Plan include steps designed to confirm that it has been consistently followed in responding to incidents during the past year.

**Management Decision: Concur**

### **Corrective Action:**

DIT's Audit and Internal Controls Section will incorporate an annual review of the Breach Response Plan as part of the CIOO Internal Control Program. The annual review will include steps to confirm that the Breach Response Plan was consistently followed in responding to incidents during the past year.

**Estimated Completion Date:** December 30, 2018

8. Define and determine the purpose of post-employment statements from former FDIC personnel and ensure the statements are consistently constructed to accomplish the defined purpose.

**Management Decision: Concur**

### **Corrective Action:**

Legal, CIOO, and DOA staffs will review the purpose, nature and content of post-employment statements from former FDIC personnel and determine, to the extent considered necessary for use in any future situations, the purpose and proper construction of such statements.

**Estimated Completion Date:** July 30, 2018

## The FDIC's Response to This Report

9. Develop guidance and training to ensure that employees and contractors are fully aware of the responsibility to return all FDIC equipment and documents and the prohibition against removing any sensitive information from FDIC premises before they depart, and understand the consequences—including available legal remedies—of providing false or inaccurate statements to the FDIC related to that responsibility.

**Management Decision: Concur**

**Corrective Action:**

The FDIC provides initial training and annual refresher training to employees and contractors on their responsibilities to protect sensitive information and Corporation equipment. All new employees and contractors sign statements indicating they will not take any FDIC business documents upon their departure. In addition, over the past several months, the forms to be signed by departing employees have been revised to emphasize the prohibition against taking FDIC business documents, and the form for contractor employees is in the process of being similarly revised. The CIOO and Legal Division (as well as DOA with respect to contractors) will review existing guidance and training to ensure that employees and contractors are fully aware of their responsibility to return all Corporation equipment and documents and the prohibition against removing any sensitive information from FDIC premises before they depart. DOA, along with the CIOO and Legal Division, will ensure that all training and guidance clearly articulate the consequences—including available legal remedies—of providing false or inaccurate statements to the FDIC related to that responsibility.

**Estimated Completion Date:** July 30, 2018

10. Ensure that its policies, procedures, and practices result in statements and representations to Congress and the American public that are full and complete and reflect the latest information known to agency personnel.

**Management Decision: Concur**

**Corrective Action:**

FDIC will update Directive 1211.2, "*Congressional Contacts and Correspondence*" to clarify and emphasize the importance of providing statements and representations to authoritative bodies that are full and complete to the best of our knowledge. Additionally, Congressional communications policies, procedures and guidelines within other divisions/offices will be reviewed to ensure they are consistent with updates to Directive 1211.2. It is FDIC's intent

## The FDIC's Response to This Report

and expectation that our policies, procedures, and practices will result in statements and representations to Congress and the American Public that are full and complete and reflect the latest information known to agency personnel.

**Estimated Completion Date:** July 30, 2018

11. Update and correct prior statements and representations made to Congress regarding the incidents addressed in this Special Inquiry where previous information is no longer accurate, valid, or complete.

**Management Decision:** Concur

**Corrective Action:**

FDIC will review and provide updated material, if necessary, to the Congress on the key incidents presented in the OIG's report using information available as of the date of the OIG's report.

**Estimated Completion Date:** July 30, 2018

12. Clarify legal hold policies and processes to ensure that all relevant personnel and sources of documents and information are included in the scope of legal holds.

**Management Decision:** Concur

**Corrective Action:**

The Legal Division commits to continuing its practice of carefully evaluating all Congressional requests to determine, based on a totality of the circumstances and subject to a reasonableness test, whether to implement a legal hold. Further, in an effort to continually improve its practices and procedures, the Legal Division launched new legal hold support software in October 2017 and is in the process of reviewing and revising *Legal Hold Directive 5500.5* and legal hold guidelines. These measures are aimed at ensuring, among other things, that relevant personnel and sources of documents and information will be included in the scope of legal holds.

**Estimated Completion Date:** July 30, 2018

13. Ensure that Congressional communications policies, procedures, and guidelines establish a single office that has accountability and authority for providing timely responses compliant with Congressional requests and communicating



## The FDIC's Response to This Report

---

with Congressional staff regarding those requests.

**Management Decision: Concur**

**Corrective Action:**

The FDIC will update Directive 1211.2 *Congressional Contacts and Correspondence*, to clarify that the Office of Legislative Affairs is the office that is responsible for providing, to the extent practicable, timely responses to Congressional requests and communicating with Congressional staff regarding those requests. Additionally, Congressional communications policies, procedures and guidelines within other divisions/offices will be reviewed to ensure they are consistent with the update to directive 1211.2.

**Estimated Completion Date:** October 30, 2018

Please contact FDIC's Division of Administration if you have any questions regarding this response. Thank you.

### The FDIC's Corrective Actions and Associated Timeframes

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved: <sup>a</sup> Yes or No	Open or Closed <sup>b</sup>
1	<p>The CIOO completed a comprehensive update of the FDIC Breach Response Plan in October 2017, which included but was not limited to clarifying the roles and responsibilities of the CISO, CIO, CPO/SAOP, and the Chairman. The CIOO will further update the Breach Response Plan to include the roles and responsibilities of FDIC's COO as part of the incident response lifecycle.</p> <p>The Chairman appointed members of the Breach Response Team and delegated in writing that the CIO/CPO is the designated signatory on notification letters sent to individuals affected by a breach. Additionally, the Breach Response Plan outlines that the Chairman is the final authority for designating a breach as a "major incident" in consultation with the CPO/SAOP and CISO, and based upon the recommendation of the Breach Response Team.</p> <p>Further, the CIOO provided training to Breach Response Team members in Q4 2017 to ensure they understood their respective roles and responsibilities at each stage of the FDIC's breach response lifecycle.</p>	June 30, 2018	N/A	Yes	Open

## The FDIC's Corrective Actions and Associated Timeframes

2	The CIOO's Audit and Internal Control Section has been tracking updates to OMB guidance and assigning any needed follow-up work to the appropriate managers within the CIOO, and will follow a similar process for Executive Orders, Binding Operational Directives, and privacy guidance. The CIOO and Audit and Internal Control Section will continue to coordinate with the Legal Division (and other divisions or offices as appropriate) to the extent necessary in determining appropriate responses to new statutory requirements and government-wide guidance. The CIOO will document the procedures for identifying, tracking, and providing guidance on the applicability and implementation of new statutory requirements and government-wide guidance.	June 15, 2018	N/A	Yes	Open
3	The Legal Division will establish procedures by which legal opinions are developed, deliberated, disseminated, and maintained. Such procedures will include the manner in which legal opinions are to be shared with divisions and offices that are stakeholders with respect to the subject matter in question, e.g., data breach management and related topics, and such opinions shall be consistent with legal, regulatory, and/or operational requirements for records management.	July 30, 2018	N/A	Yes	Open
4	The October 2017 version of the Breach Response Plan includes distinct decision paths for	December 31, 2017	N/A	Yes	Closed

## The FDIC's Corrective Actions and Associated Timeframes

	consumer notification and credit monitoring. In November and December 2017, the CIOO provided training to the Breach Response Team members that addressed (among other things) the distinct decision paths for consumer notification and credit monitoring.				
5	<p>In December 2016, RMS issued a memorandum that included a requirement to immediately notify FinCEN concerning any apparent, threatened, or possible BSA data compromise or loss. RMS shared this requirement with examiners and other RMS staff through the memorandum and multiple conference calls. RMS will continue to provide reminders to all staff annually that information maintained in, or available through, the FinCEN database is sensitive – and in some instances confidential – and may only be retrieved and used for official FDIC business.</p> <p>RMS will continue to coordinate with the CIOO and the Legal Division as appropriate, particularly with respect to the responsibility and timeframes for reporting incidents to FinCEN where SAR information has been compromised. In addition, in May 2018, RMS will issue a global email reminder regarding the requirement to report incidents to FinCEN when SAR information has been compromised.</p>	June 30, 2018	N/A	Yes	Open
6	The October 2017 version of the Breach Response Plan requires that an annual breach response tabletop exercise be performed.	December 13, 2017	N/A	Yes	Closed

## The FDIC's Corrective Actions and Associated Timeframes

	<p>Pursuant to the Breach Response Plan, the key members of Breach Response Team are required to participate in the breach response tabletop exercise. In December 2017, a breach response tabletop exercise was completed to test the new plan and ensure that members of the Breach Response Team were familiar with the plan and understand their specific roles. Furthermore, as provided in the Breach Response Plan, those key officials designated as members of the Breach Response Team will continue to participate in future breach response tabletop exercises.</p>				
7	<p>DIT's Audit and Internal Controls Section will incorporate an annual review of the Breach Response Plan as part of the CIOO Internal Control Program. The annual review will include steps to confirm that the Breach Response Plan was consistently followed in responding to incidents during the past year.</p>	December 30, 2018	N/A	Yes	Open
8	<p>Legal, CIOO, and DOA staffs will review the purpose, nature, and content of post-employment statements from former FDIC personnel and determine, to the extent considered necessary for use in any future situations, the purpose and proper construction of such statements.</p>	July 30, 2018	N/A	Yes	Open
9	<p>Over the past several months, the FDIC has revised the forms to be signed by departing employees to emphasize the prohibition against taking FDIC business documents, and the</p>	July 30, 2018	N/A	Yes	Open

## The FDIC's Corrective Actions and Associated Timeframes

	<p>form for contractor employees is in the process of being similarly revised. The CIOO and Legal Division (as well as DOA with respect to contractors) will review existing guidance and training to ensure that employees and contractors are fully aware of their responsibility to return all Corporation equipment and documents and the prohibition against removing any sensitive information from FDIC premises before they depart. DOA, along with the CIOO and Legal Division, will ensure that all training and guidance clearly articulate the consequences—including available legal remedies—of providing false or inaccurate statements to the FDIC related to that responsibility.</p>				
10	<p>The FDIC will update Circular 1211.2, <i>Congressional Contacts and Correspondence</i>, to clarify and emphasize the importance of providing statements and representations to authoritative bodies that are full and complete to the best of the FDIC's knowledge. Additionally, Congressional communications policies, procedures, and guidelines within other divisions/offices will be reviewed to ensure they are consistent with updates to Circular 1211.2.</p>	July 30, 2018	N/A	Yes	Open
11	<p>The FDIC will review and provide updated material, if necessary, to Congress on the key incidents presented in the OIG's report using information available as of the date of the OIG's report.</p>	July 30, 2018	N/A	Yes	Open

## The FDIC's Corrective Actions and Associated Timeframes

12	The Legal Division commits to continuing its practice of carefully evaluating all Congressional requests to determine, based on a totality of the circumstances and subject to a reasonableness test, whether to implement a legal hold. Further, in an effort to continually improve its practices and procedures, the Legal Division launched new legal hold support software in October 2017 and is in the process of reviewing and revising Circular 5500.5 and the legal hold guidelines. These measures are aimed at ensuring, among other things, that relevant personnel and sources of documents and information will be included in the scope of legal holds.	July 30, 2018	N/A	Yes	Open
13	The FDIC will update Circular 1211.2 to clarify that OLA is the office that is responsible for providing, to the extent practicable, timely responses to Congressional requests and communicating with Congressional staff regarding those requests. Additionally, Congressional communications policies, procedures, and guidelines within other divisions/offices will be reviewed to ensure they are consistent with the update to Circular 1211.2.	October 30, 2018	N/A	Yes	Open

<sup>a</sup> Recommendations are resolved when —

1. Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.

## The FDIC's Corrective Actions and Associated Timeframes

---

2. Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no (\$0) amount. Monetary benefits are considered resolved as long as management provides an amount.

<sup>b</sup> Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.





Federal Deposit Insurance Corporation  
Office of Inspector General

---

3501 Fairfax Drive  
Room VS-E-9068  
Arlington, VA 22226

(703) 562-2035

☆☆☆☆☆

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our [Hotline](#) or call 1-800-964-FDIC.

---

FDIC OIG website

[www.fdicigo.gov](http://www.fdicigo.gov)

Twitter

@FDIC\_OIG

OVERSIGHT.GOV  
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

[www.oversight.gov/](http://www.oversight.gov/)