



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 (202) 898-3888 or Andy Jiminez, Director of the Office of Legislative Affairs, at (202) 898-6761.

Sincerely,

Martin J. Gruenberg

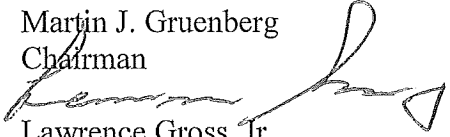
Enclosure

cc: Honorable Eddie Bernice Johnson, Ranking Member



May 9, 2016

MEMORANDUM TO: Martin J. Gruenberg  
Chairman

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.

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.

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.

**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.