Division of Supervision and Consumer Protection

MEMORANDUM SYSTEM

Classification Number:	6600
Date:	August 15, 2006
Issuing Office:	Technology Supervision Branch
Contact:	Michael Jackson 202-898-6748 Jaime Perez 202-898-6653
☐ Notice	☒ Memorandum

MEMORANDUM TO: Regional Directors

FROM: Sandra L. Thompson
Acting Director

SUBJECT: Safeguarding Examination Information

1. **Purpose.** To remind staff of the importance of safeguarding examination information whether in paper, electronic, or other form.

2. **Background.** Examination information is broadly defined as all documentation involved in a bank examination. It includes the Report of Examination (ROE), examination work papers, and bank information received during the examination process. Examination information requested from the bank may contain non-public, sensitive bank customer information as defined in Section 501(b) of the Gramm-Leach-Bliley Act, such as social security numbers, personal identification numbers, and account numbers. Inherent risks to this information include theft, loss, or unauthorized access. Therefore, access, storage and transport of examination information stored on laptops, retained on compact disks (CDs), digital video disks (DVDs), flash drives, or any other storage media, and hard copies of ROEs and examination work papers requires the highest level of confidentiality and must be safeguarded to prevent misuse and to minimize legal and reputational risks to the FDIC.

3. **Action.** Staff is reminded to exercise strong internal control processes to protect against any threats or hazards to the security or confidentiality of examination information. Staff must adhere to all directives or memoranda governing the use and security of any confidential examination information acquired or created during the examination process, and during the course of normal business operations.

4. **Effective Date.** This memorandum is effective immediately.

5. **Distribution.** Regional Directors should ensure that this memorandum is distributed to all DSC staff.

Attachments: Attachment A
Attachment B

Transmittal No.: 2006-025

Attachment A

The recent high profile information security breaches reported in the press have prompted the Division of Supervision and Consumer Protection to remind management and staff of the importance of safeguarding examination information. Each employee should understand their responsibility to protect examination information and to abide by outstanding federal and FDIC corporate guidelines.

Refer to the following Regional Director Memorandum entitled:

- Safekeeping of Confidential Records, dated September 5, 1997, #97-067.
- Security of Electronic Data Acquired or Created During the Examination Process, dated November 19, 2002, #02-046.
- E-Exam Policy, dated July 7, 2006, #06-17.

The Division of Information Technology also provides the following rules on:
Protecting Sensitive Information on their internal website.

Safeguarding Examination Information

FDIC regional offices shall develop procedures to protect examination information when it is accessed, transported, stored, and disposed of. Access to examination information includes both securing physical access (i.e. files rooms) and electronic access (i.e. password protection). Securing the transport of examination information includes both electronic transmissions (i.e. encrypting e-mail) and securing physical transport (i.e. automobile or commercial carrier). The storage of examination information includes securing both physical and electronic sources of storage. The protection of examination information will require technical, physical, and administrative safeguards. Minimum standards include:

Technical:

1. All examination information stored on laptops, retained on CDs, DVDs, flash drives, or any other storage media shall be encrypted.
2. All e-mails containing confidential information must be encrypted.
3. All computer passwords must be kept secure, which means not near or on your computer.
4. All computer passwords must (1) be at least eight characters long, (2) not spell a word, (3) use both the alphabet and numbers, and (4) include at least three of the following: one lowercase alphabetic character, one uppercase alphabetic character, one numeric character or special character (!@#$%^&*).

Physical:

1. Ensure unattended computers and other approved portable computing devices are physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system. When traveling by automobile, laptops should be secured in the car trunk.
2. Electronic and hard copies of ROEs and examination work papers shall be stored in locked filing areas.
3. Financial institutions may submit information electronically to approved recipients within the FDIC if the data is encrypted and subsequently protected (refer to FDIC Circular 1310.5 –

Encryption and Digital Signatures for Electronic Mail). Institutions should be strongly encouraged to provide information securely to the FDIC via FDIC*connect*.

4. All examination work papers and other confidential information should be physically stored and transported securely at all times.
5. When transporting work papers (either by personally-owned vehicle or commercial carrier), maintain a list of specific items containing bank customer information and any other confidential information separate from the work papers in the event of theft or loss.
6. Regional procedures shall be developed to track the transport of work papers and ensure timely receipt of all shipments. These procedures should clearly indicate the person responsible for verifying receipt of shipped examination information, labeling procedures including sender and receiver's address and telephone number, and instructions for including sender and receiver information inside the package.
7. Copying documents containing confidential bank customer information for work papers should be discouraged. For example, copying information from bank customer loan applications and tax returns for credit analysis purposes should be discouraged. Necessary numbers from these documents should be transcribed to loan tabs. In the event that there is no alternative, the work papers should be marked confidential and properly disposed of as soon as work paper retention periods expire.
8. Staff on travel status or telework status must ensure confidential information is secure when unattended.

Administrative:

1. Regional Directors and their designees shall have responsibility for information security of regional and field offices.
2. Regional offices will provide periodic training on information security procedures.

Information Security Incident Response Programs

DSC will implement an Information Security Incident Response Program to address incidents of lost, stolen, or unauthorized access of confidential examination information. The plan will address regional and field office locations. The program will specify actions to be taken when a DSC employee suspects or detects that examination information has been compromised. The regional and field offices are encouraged to add an addendum addressing unique circumstances at their locations.

As part of DSC's incident response program the regional offices shall:

1. Identify reasonably foreseeable internal and external threats to confidential information.
2. Assess the likelihood and potential damage of these threats.
3. Assess the sufficiency of policies and procedures to control these risks.
4. Develop measures to protect against loss or theft of confidential information.
5. Develop incident response programs that specify actions the FDIC will take when it detects or suspects that confidential information has been compromised.

DSC's incident response program shall contain regional procedures to adequately address the following:

1. Assess the nature and scope of the incident.
2. Notify appropriate management contacts as quickly as possible and in all cases within one hour of discovery of actual or suspected loss of examination information.

3. Take appropriate steps to contain and control the incident.
4. Notify the financial institution of an incident involving examination information, after completing a reasonable investigation.

Regional Directors have the authority and discretion when warranted, to pay certain costs: (i.e. customer notification) after a reasonable investigation by bank management, determines customer notification is warranted. When this cost is expected to exceed authorization limits the Regional Director should contact the Deputy Director of Strategic Planning and Resource Management. Authority to pay certain costs does not include authorizing indemnification against possible loss, damage, or liability.

Attachment B

From: Global Messenger
Sent: Tuesday, August 08, 2006 4:49 PM
To: FDIC EMPLOYEES CORPORATE; CONTRACTORS CORPORATE
Subject: Revised: Update on Protecting Sensitive Data

TO: All Employees and Contractors

FROM: Michael E. Bartell
Chief Privacy Officer

DATE: August 8, 2006

SUBJECT: Revised Update on Protecting Sensitive Data

This message supersedes the Global Email message issued on July 26, 2006, regarding interim FDIC policy on protecting sensitive data and is intended to give guidance on the subject until issuance of an FDIC Circular currently in preparation.

Notification of Loss

FDIC policy requires any suspected loss of sensitive information be reported immediately to the FDIC's Help Desk which is staffed 24 hours a day, seven days a week. The Office of Management and Budget (OMB) has now issued a directive requiring all federal agencies to report all incidents of a confirmed or suspected loss of Personally Identifiable Information (PII) within one hour of discovering the incident. PII includes any personal information maintained by an agency about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other information that is linked or linkable to the individual.

If you know of or suspect a loss of sensitive information involving PII, whether in electronic or hard copy format, it is essential that users report the incident to the FDIC's Help Desk 1-877-FDIC-999 (1-877-334-2999) immediately. This will provide the FDIC time to gather critical information concerning the incident, notify the appropriate FDIC management and report the incident as required by OMB. You should also notify your supervisor/oversight manager and your division/office Information Security Manager (ISM) at the earliest possible opportunity.

Reminder on Privacy Act Requirements

The Privacy Act of 1974 addresses requirements for the appropriate collection, maintenance, use and/or dissemination of records that are subject to the Act, i.e., records maintained in a privacy act "system of records" (the FDIC public Web site contains a list of Privacy Act systems of records maintained by FDIC). In addition, FDIC Circular 1031.1, Administration of the Privacy Act, provides guidance for the appropriate collection, maintenance, use and/or dissemination of records (data) subject to the Privacy Act ("Records"), including:

- Collect only Records that are relevant and necessary to accomplish an authorized FDIC function, and do so directly from the individual whenever possible.

- Inform individuals what Records are being collected, why they are being collected, and of their right to review and update the information as authorized by law.

- Do not disclose Records unless the requestor has received prior permission from the subject of the Records, disclosure is made subject to published routine use, or disclosure is otherwise authorized by law.

The foregoing precautions do not inhibit obtaining and using information obtained in connection with an examination, litigation, investigation, bank failure, or other legitimate FDIC activity in ways that are otherwise lawful, such as by sharing information with law enforcement or regulatory agencies in appropriate circumstances.

Other Safeguards

In addition, the following summarizes additional responsibilities involving sensitive information and I encourage everyone to read and fully apply this guidance:

- Protect any PII collected from unauthorized access. Do not access PII unless you have a legitimate need to do so in the performance of your duties.

- Do not remove PII from the workplace unless necessary for the performance of your duties, and if it must be removed, ensure it is kept secure at all times. This includes encrypting the data if it is on a laptop or other portable media, such as a CD or flash drive, and keeping paper reports or output in a secure area, such as a locked office or file cabinet.

- Do not access PII remotely unless necessary for the performance of your duties and ensure the access connection is secure.

- Encrypt PII whenever possible. This includes always encrypting such data when it is stored on a laptop or on removable media as well as when it is transmitted by e-mail, except when the requirement of email encryption is not possible and it would prevent the execution of an essential FDIC function or activity.

- If sensitive data or PII must be sent by e-mail, it should be sent over a secure link whenever possible, such as via e-mail exchanged within the FDIC e-mail system, e-mail sent via the secure link with many of the state banking agencies (using TLS), or e-mail sent across the secure path between the FDIC and the Office of Thrift Supervision (OTS) or the Office of the Comptroller of the Currency (OCC). Where possible, such data should also be encrypted. Avoid the use of unsecured links when transmitting PII, except when encryption is not possible and it would prevent the execution of an essential FDIC function or activity.

- If sensitive data or PII must be sent by the postal service or by commercial carrier, the shipment should be tracked using a tracking number and the sender should follow up in a timely manner to ensure that the item has been properly received. If possible, the shipment should require an authorized signature upon delivery. Items should be sealed in a fully addressed container (including

the sender's return address and telephone number). Also, inside the container, the sender should clearly mark the material as "sensitive" and include the sender's return address and telephone number. Maintain a list of the specific items containing PII included in the shipment to assist in follow up activities in case they are lost or stolen. If the material being shipped is electronic media, explore the possibility of encrypting it.

- When sensitive data or PII must be provided by institutions being examined by FDIC, the exchange of information must be done securely. Institutions should be strongly encouraged to provide the data securely via FDIC*connect*.

- Secure hard copies of PII until properly disposed of. Promptly retrieve output from printers, safeguard hard copies in your work area, and shred them or place them in locked shred bins when they are no longer needed.

As employees and contractors who may have access to PII, you play a role in enforcing and have a responsibility to comply with the FDIC's privacy policy in order to protect PII maintained or used by the Corporation. Additional information about FDIC's Privacy Program can be found on the FDIC public Web site. Questions should be directed to Ned Goldberg, Chief Information Security Officer, at 703-516-1323 or NGoldberg@FDIC.gov.