* Pedestrian changes have been made to the directive and appear in blue. 7/27/2015, 5/14/2014, 5/28/2013, and 10/27/2015.)

FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1360.9	
CONTACT	TELEPHONE NUMBER
Christopher Farrow	(703) 516-5507
DATE	
April 30, 2007	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All Divisions and Offices

FROM: Martin D. Henning
Acting Chief Information Officer and Chief Privacy Officer
Chief Information Officers Organization

SUBJECT: Protecting Sensitive Information

1. Purpose

To establish FDIC policy on protecting sensitive information collected and maintained by the Corporation and to provide guidance for safeguarding the information.

2. Scope

The provisions outlined in this circular apply to all employees and contractors as well as any other persons who have access to sensitive information used in the performance of Corporation business. This includes data maintained electronically as well as information available in hard copy (paper) format.

3. Background

Interim guidance on Protecting Sensitive Information was provided by the Chief Information Officer/Chief Privacy Officer in a global electronic mail (email) message to employees dated August 8, 2006.

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 (FOIA) and information whose disclosure is governed by the Privacy Act of 1974 (Privacy Act). Sensitive information requires a high level of protection from loss, misuse, and unauthorized access or modification. Failure to protect sensitive information may cause the Corporation to be in violation of the law or may result in avoidable costs or damage to the FDIC's reputation. See paragraph 4.c., below for a more detailed definition of sensitive information.

In recent years, the increase in the incidence of identity fraud has focused attention on protecting the privacy of individuals by both commercial businesses and government agencies. In the role as an employer and in support of its mission, the Corporation collects and maintains information about employees and other individuals as well as information obtained from other sources including insured institutions and the institutions' customers. Accordingly, the Corporation has a

Background (cont.)

responsibility to protect this personally identifiable information (PII). See paragraph 4.b., below for a more detailed definition of PII. PII is also sometimes referred to as information in identifiable form (IIF).

Throughout this circular, the term **sensitive information** applies to the broad range of information requiring protection.

---

4. Definitions

Terms specific to this circular are defined below:

a. **Information in Identifiable Form (IIF)**. See Personally Identifiable Information.

b. **Personally Identifiable Information (PII)**. Any information about an individual maintained by FDIC which 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 (SSN), 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 which is linked or linkable to an individual.

c. **Sensitive information**. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. It includes, but not exclusively, the following:

(1) Information that is exempt from disclosure under the Freedom of Information Act (FOIA) such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel and medical files, and information contained in bank examination reports (see FDIC Rules and Regulations, 12 C.F.R. Part 309, for further information);

(2) Information under the control of FDIC contained in a Privacy Act system of record that is retrieved using an individual's name or by other criteria that identifies an individual (see FDIC Rules and Regulations, 12 C.F.R. Part 310, for further information);

(3) PII about individuals maintained by FDIC that if released for unauthorized use may result in financial or personal damage to the individual to whom such information relates. Sensitive PII, a subset of PII, may be comprised of a single item of information (e.g., SSN) or a combination of two or more items (e.g., full name along with,

Definitions (cont.)

financial, medical, criminal, or employment information). Sensitive PII presents the highest risk of being misused for identity theft or fraud;

(4) Information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities; and

(5) Information related to information technology specific to the FDIC that could be misused by malicious entities (e.g., firewall rules, encryption and authentication mechanisms, and network architecture pertaining to the FDIC).

(6) Except as required in electronic mail, internal IP addresses and server names must be encrypted if they are sent outside of the FDIC.

---

5. Policy

In order to protect sensitive information, it is the policy of the FDIC to:

a. Collect and retain sensitive information only when it is necessary to satisfy an FDIC business requirement;

b. Identify the existence of sensitive information in both electronic and paper formats by labeling removable electronic media (e.g., diskettes, CD/DVD, USB flash drives) and paper reports (on the cover page and/or in the footer section) as containing sensitive information;

c. Safeguard sensitive information from unauthorized access. Only those individuals who have a legitimate need to access sensitive information in the performance of their duties shall be provided access;

d. Store sensitive electronic information only on corporate information technology (IT) equipment. Store paper copies in corporate facilities (e.g., locked drawers, file cabinets, and file rooms) whenever possible;

Note: Sensitive information shall not be removed from the workplace without prior management approval, and if it must be removed, it shall be kept secured at all times. Whether in electronic or paper format, it shall not be left unattended unless properly physically secured.

e. Encrypt sensitive information stored on end-user IT equipment (e.g., laptop and desktop computers) as well as on removable media (e.g., diskettes, CD/DVD, USB flash drives);

f. Remotely access sensitive information stored in electronic format only across a secure connection, such as via remote access services supported by the Corporation;

Policy (cont.)

g. Send sensitive information electronically only when required. Email messages containing sensitive information shall always be encrypted using an FDIC-approved encryption product. See Encryption Guidance on FDICnet for further information. External parties must follow the most current encryption guidance and Federal Information Processing Standards (FIPS) for encryption published by the National Institute of Standards and Technology (NIST). Further, personal email accounts (e.g., Gmail or Hotmail) should never be used for transmitting or receiving any type of sensitive FDIC business-related information;

h. Ship sensitive information by postal service or commercial carrier only when required. The shipment shall be tracked and followed up on in a timely manner to ensure that it arrives intact at its destination. See the Division of Administration (DOA) Express Mail Job Aid on FDICnet for minimum requirements for shipping sensitive materials (paper and/or electronic);

i. Properly dispose of electronic media and paper documents containing sensitive information when they are no longer needed (and in accordance with records retention requirements). **Electronic media and paper documents shall not be discarded intact in a trash can**. Paper documents shall be shred (or placed in a shred bin provided by the Corporation) and electronic storage media shall be destroyed (or placed in an electronic media console provided by the Corporation). See Protecting Sensitive Information in Your Work Area A Guide for the FDIC on FDICnet for further information; and

j. Require all employees and contractors to complete annual security and privacy awareness training.

In the event that sensitive data is suspected or known to be lost or otherwise compromised, whether in electronic or paper format, report the situation **immediately** to the FDIC Help Desk/Computer Security Incident Response Team (CSIRT) (877-FDIC-999). Also notify your supervisor/oversight manager and your division/office Information Security Manager at the earliest available opportunity. Search "ISM Program" on FDICnet for a list of current Information Security Managers.

6. Guidelines

Because a significant portion of the FDIC workforce is mobile, safeguarding sensitive information presents an ongoing challenge. The following guidelines provide additional information intended to assist employees and contractors in their continuous efforts to protect sensitive information:

a. Maintain physical control over sensitive information stored electronically. Keep portable IT equipment (laptops, personal digital assistants (PDAs), USB flash drives, CDs/DVDs, diskettes, etc.) with you at all times and avoid leaving them unattended.

Guidelines (cont.)

(1) If you must leave portable IT equipment such as a laptop in a vehicle, store it in the trunk or out of sight in the passenger compartment and lock the vehicle. Be aware of others watching you place it in the vehicle. Do not leave IT equipment in a vehicle overnight or for long periods of time – keep it with you.

(2) Do not leave portable IT equipment unattended when traveling. Monitor it closely while checking in at an airport or hotel counter and while passing through airport security checkpoints. If you must leave IT equipment briefly unattended in a hotel room, store it out of sight, in a room safe if one is provided, or secure it to a desk or table with a cable lock. (Laptop cable locks are available from DIT upon request).

(3) When traveling by air, bring the portable IT equipment with you on the airplane as a carry-on. Do not place it in checked luggage.

(4) Do not leave portable IT equipment unattended at a conference, convention, or other public event; carry items with you at all times. Alternatively, secure a laptop to a desk or table with a cable lock.

(5) Do not leave portable IT equipment unattended in the workplace. When not in use, secure it in a locked drawer or room.

If necessary, secure a laptop to a desk or table with a cable lock, especially in non-FDIC facilities.

b. Maintain physical control over sensitive information stored in paper format.

(1) When not in use, store documents containing sensitive information in locked file drawers or a secured room.

(2) When making copies of documents containing sensitive information, remember to retrieve the originals and all copies from the copier.

(3) Retrieve documents containing sensitive information from shared printers as soon as they are printed. When available, print to printers located in secured rooms.

(4) When faxing documents containing sensitive information, promptly retrieve the original from the sending fax machine and alert the recipient to promptly retrieve the copy from the receiving fax machine. When expecting a faxed document containing sensitive information, monitor the fax machine closely and retrieve the fax as soon as it arrives. When available, use fax machines located in secured rooms.

Guidelines (cont.)

(5) When documents containing sensitive information are no longer needed on-site, transfer them to an off-site records center or shred them before discarding (or place them in a shred bin provided by the Corporation). **Do not place them intact in a trash can**.

c. Utilize encryption for both the storage of electronic files on IT equipment (e.g., laptop, desktop) and for the transmission of files, such as by email. Different encryption solutions are available to support these requirements. See Encryption Guidance on FDICnet for further information. External parties must follow the most current encryption guidance and Federal Information Processing Standards (FIPS) for encryptions published by the National Institute of Standards and Technology (NIST).

d. Send email containing sensitive information using approved secure solutions:

(1) For internal messages within the Corporation, encrypt the message using encryption software provided within the corporate email program. See Encryption Guidance on FDICnet for further information.

(2) For external messages destined for non-FDIC recipients, use approved encryption solution(s). See Encryption Guidance on FDICnet for further information.

e. Improve the level of protection when physically shipping IT equipment or documents containing sensitive information by interoffice mail, postal service, or commercial carrier. See the Division of Administration (DOA) Express Mail Job Aid on FDICnet for minimum requirements for shipping sensitive materials (paper and/or electronic).

f. Follow the procedures outlined in the FDIC Data Breach Handling Guide available on the FDICnet for incidents involving the loss, misuse or unauthorized access of SI and/or PII in either electronic or paper format in order to reduce the potential for harm or embarrassment to the individual and the Corporation.

7. Responsibilities

a. **Employees and contractors** shall:

(1) Protect sensitive information as outlined in this circular;

(2) Immediately notify the DIT Help Desk in the event they suspect or know that sensitive information is lost or otherwise compromised, with follow-up notification to their supervisor/oversight manager and division/office Information Security Manager at the earliest available opportunity; and

(3) Complete security and privacy awareness training on an annual basis.

Responsibilities (cont.)

b. **Supervisors and Oversight Managers** shall:

(1) Assist their employees and contractors in identifying sensitive information in the workplace and ways to safeguard such information appropriately; and

(2) Participate in the development and execution of a corporate response plan in the event of loss or compromise of sensitive data.

c. Division/Office **Information Security Managers** shall:

(1) Help to ensure that sensitive information is adequately protected through their participation in FDIC's Information Security Risk Management Program; and

(2) Assist in the development and execution of a corporate response plan in the event of loss or compromise of sensitive data.

d. The **DIT Help Desk** shall serve as a central point of contact, available 24 hours a day, seven days a week, for receiving notification of lost or compromised sensitive information and alerting the DIT Computer Security Incident Response Team (CSIRT).

e. The DIT **Computer Security Incident Response Team (CSIRT)** shall:

(1) Collect facts and document all incidents involving loss or compromise of sensitive information;

(2) Notify appropriate technical staff, senior management, and Office of Inspector General (particularly if there is suspected violation of criminal law) about an incident involving loss or compromise of sensitive information so that prompt action may be taken;

(3) Participate in the development and execution of a corporate response plan in the event of loss or compromise of sensitive data; and

(4) Notify the United States Computer Emergency Readiness Team (US-CERT) within one hour of the incident if it involves the loss or compromise of PII.

f. The **Chief Information Officer/Chief Privacy Officer** shall:

(1) Play a central role in developing and maintaining policy and procedures in the area of privacy and the protection of sensitive information;

Responsibilities (cont.)	(2) Prepare reports to Congress and to the Office of Management and Budget on activities related to privacy and the protection of sensitive information as required by law, regulation, or directive; (3) Perform, direct, or ensure reviews of privacy or other sensitive information as required by law, regulation, or directive; (4) Oversee the Data Breach Management Team (DBMT) activities in assessing high risk incidents involving SI and/or PII and recommending a course of action.
8. Disciplinary Action	Employees or contractors who violate the provisions of this policy may be subject to disciplinary action up to and including removal from Federal service or from their contract. Any disciplinary action will be administered in accordance with applicable law, regulations, FDIC policies and procedures, contractual agreements, and applicable collective bargaining agreements.
9. Recordkeeping Requirements	Dispose of electronic media and paper documents in accordance with FDIC Circular 1210.1, FDIC Records and Information Management (RIM) Policy Manual.
10. References	For additional information regarding protecting sensitive information, refer to the following: a. FDIC Privacy Program (www.fdic.gov/about/privacy). b. FDIC Rules and Regulations – Disclosure of Information, 12 C.F.R. Part 309. c. FDIC Rules and Regulations – Privacy Act Regulation, 12 C.F.R. Part 310. d. FDIC Circular 1023.1, Procedures for Processing Freedom of Information Act Requests. e. FDIC Circular 1031.1, Administration of the Privacy Act. f. FDIC Circular 1360.12, Reporting Computer Security Incidents. g. FDIC Circular 1360.16, Mandatory Information Security Awareness Training. h. FDIC Data Breach Handling Guide i. Privacy Act of 1974, 5 U.S.C. § 552a.

References (cont.)

j. Freedom of Information Act, 5 U.S.C. § 552.

k. Office of Management and Budget Circular No. A-130, Management of Federal Information Resources

l. Paperwork Reduction Act of 1995, 44 U.S.C. § 3501.

m. E-Government Act of 2002, Pub. L. No. 107-347.

n. Consolidated Appropriations Act, 2005, § 522, Pub. L. No. 108-447.

o. Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

p. Office of Management and Budget Memorandum M-06-15, Safeguarding Personally Identifiable Information.

q. Office of Management and Budget Memorandum M-06-16, Protection of Sensitive Agency Information.

r. Office of Management and Budget Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.

s. Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

t. FDIC Circular 1360.19, Privacy Impact Assessment Requirements

u. FDIC Circular 1360.20, FDIC Privacy Program

11. Effective Date The provisions outlined in this circular are effective immediately.