Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-56-2010
September 15, 2010

GUIDANCE ON MITIGATING RISK POSED BY INFORMATION STORED ON PHOTOCOPIERS, FAX MACHINES AND PRINTERS

Summary: The FDIC has issued the attached guidance, which describes the risk posed by sensitive information stored on certain electronic devices and how institutions should mitigate that risk.

Suggested Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Compliance Officer
Chief Information Security Officer

Related Topics:

- FIL-100-2007, Identity Theft Red Flags, November 15, 2007
- FIL-32-2007, Identity Theft, FDIC's Supervisory Policy on Identity Theft, April 11, 2007
- FIL-7-2005, Guidelines Requiring the Proper Disposal of Consumer Information, February 2, 2005
- FIL-22-2001, Guidelines Establishing Standards for Safeguarding Customer Information, March 14, 2001

Attachment:
FDIC Guidance on Mitigating Risk Posed by Information Stored on Photocopiers, Fax Machines and Printers

Contact:
Jeffrey Kopchik, Senior Policy Analyst, at jkopchik@fdic.gov or (202) 898-3872

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2010/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- Photocopiers, fax machines and printers may contain a hard drive or flash memory that stores digital images of documents that are copied, transmitted or printed by the device.
- These digital images may contain sensitive and confidential information concerning financial institution customers.
- Financial institutions should implement written policies and procedures to ensure that a hard drive or flash memory containing sensitive information is erased, encrypted or destroyed prior to the device being returned to the leasing company, sold or otherwise disposed of.

FDIC GUIDANCE ON MITIGATING RISK POSED BY INFORMATION STORED ON PHOTOCOPIERS, FAX MACHINES AND PRINTERS

This guidance describes the risk posed by sensitive information stored on certain electronic devices and how institutions should mitigate that risk.

Risk

Photocopiers, fax machines and printers may contain a hard drive or flash memory that stores digital images of the documents that are copied, transmitted or printed by the device. Financial institutions use these devices regularly to process loans and other financial transactions on behalf of their customers. Loan documents and other business documents often contain sensitive and confidential information concerning financial institution customers.

Many financial institutions lease photocopiers, fax machines and printers for a set period of time. At the end of the lease period, the devices are returned to the leasing company and either sold or leased again. Anyone who takes subsequent possession of a device that was used by a financial institution may be able to access the hard drive or flash memory and view digital images of the documents that were processed by the device, thus giving them access to sensitive personal and business information concerning the institution's customers.

Controls

Financial institutions should be aware of the risks posed by the potential disclosure of sensitive customer information stored on the hard drive or flash memory of photocopiers, fax machines and printers used by the institution. Financial institutions should implement written policies and procedures to identify devices that store digital images of business documents and ensure their hard drive or flash memory is erased, encrypted or destroyed prior to being returned to the leasing company, sold to a third party or otherwise disposed of. If the institution chooses to erase or encrypt the hard drive, the method used should be sufficiently robust to render the information on the disk unrecoverable.[1] Examiners may ask to review such policies and procedures and verify that they have been effectively implemented.

Further Information

For further information, contact Jeffrey Kopchik, Senior Policy Analyst, at (202)-898-3872 or jkopchik@fdic.gov.

[1] See Interagency Guidelines Establishing Information Security Standards, 12 CFR 364, Appendix B, Sections II, B, 4; III, C, 4.