

- Inform the customer about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft, and encourage the customer to report any incidents of identity theft to the FTC. The notice should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.¹⁹

Optional Element: Institutions also may wish to provide customers with the following additional assistance that other institutions have offered under these circumstances:

- Provide a toll-free telephone number that customers can call for assistance;
- Offer to assist the customer in notifying the nationwide credit reporting agencies of the incident and in placing a fraud alert in the customer's consumer reports; and
- Inform the customer about subscription services that provide notification anytime there is a request for the customer's credit report or offer to subscribe the customer to this service, free of charge, for a period of time.

The institution may also wish to include with the notice a brochure regarding steps a consumer can take to protect against identity theft, prepared by the Agencies that can be downloaded from the Internet.²⁰

III. Circumstances for Customer Notice

Standard for Providing Notice

An institution should notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity.

Sensitive Customer Information

Under the Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to sensitive customer information because this type of information is easily misused, as in the commission of identity theft. For purposes of this Guidance, sensitive customer information means a customer's social security number, personal identification number, password or account number, in conjunction with a personal identifier such as the customer's name, address, or telephone number. Sensitive customer information would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such

as user name and password. Therefore, institutions are expected to notify affected customers when sensitive customer information has been improperly accessed, unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers.

Examples of When Notice Should Be Given

An institution should notify affected customers when it is aware of the following incidents unless the institution, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers:

- An employee of the institution has obtained unauthorized access to sensitive customer information maintained in either paper or electronic form;
- A cyber intruder has broken into an institution's unencrypted database that contains sensitive customer information;
- Computer equipment such as a laptop computer, floppy disk, CD-ROM, or other electronic media containing sensitive customer information has been lost or stolen;
- An institution has not properly disposed of customer records containing sensitive customer information; or
- The institution's third party service provider has experienced any of the incidents described above, in connection with the institution's sensitive customer information.

Examples of When Notice Is Not Expected

An institution is not expected to give notice when it becomes aware of an incident of unauthorized access to customer information, and the institution, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers. For example, an institution would not need to notify affected customers in connection with the following incidents:

- The institution is able to retrieve sensitive customer information that has been stolen, and reasonably concludes, based upon its investigation of the incident, that it has done so before the information has been copied, misused or transferred to another person who could misuse it;
- The institution determines that sensitive customer information was improperly disposed of, but can establish that the information was not retrieved or used before it was destroyed;
- A hacker accessed files that contain only customer names and addresses; or
- A laptop computer containing sensitive customer information is lost, but the data is encrypted and may only be accessed with a secure token or similarly secure access device.

Dated: July 31, 2003.

Mark J. Tenhundfeld.

Assistant Director, Office of the Comptroller of the Currency.

By the Board of Governors of the Federal Reserve System on August 5, 2003.

Jennifer J. Johnson,

Secretary of the Board.

Dated: August 6, 2003.

Michael J. Zamorski,

Director, Division of Supervision and Consumer Protection, Federal Deposit Insurance Corporation.

Dated: July 30, 2003.

James E. Gilleran,

Director.

[FR Doc. 03-20440 Filed 8-11-03; 8:45 am]

BILLING CODE 6720-01-P; 4810-33-P; 6210-1-P; 6714-01-P

DEPARTMENT OF THE TREASURY

Internal Revenue Service

Proposed Collection; Comment Request for Form 5558

AGENCY: Internal Revenue Service (IRS), Treasury.

ACTION: Notice and request for comments.

SUMMARY: The Department of the Treasury, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995, Pub. L. 104-13 (44 U.S.C. 3506(c)(2)(A)). Currently, the IRS is soliciting comments concerning Form 5558, Application for Extension of Time To File Certain Employee Plan Returns.

DATES: Written comments should be received on or before October 14, 2003 to be assured of consideration.

ADDRESSES: Direct all written comments to Glenn Kirkland, Internal Revenue Service, room 6411, 1111 Constitution Avenue NW., Washington, DC 20224.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the form and instructions should be directed to Larnice Mack at Internal Revenue Service, room 6407, 1111 Constitution Avenue NW., Washington, DC 20224, or at (202) 622-3179, or through the Internet at Larnice.Mack@irs.gov.

SUPPLEMENTARY INFORMATION:

Title: Application for Extension of Time To File Certain Employee Plan Returns.

¹⁹ Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are <http://www.ftc.gov/idtheft> and 1-877-IDTHEFT.

²⁰ <http://www.occ.treas.gov/idtheft.pdf>; <http://www.federalreserve.gov/consumers.htm>; <http://www.fdic.gov/consumers/consumer/news/csum00/idthft.html>; <http://www.ots.treas.gov/docs/25139.pdf>.