

comments and the related index on the OTS Internet Site at <http://www.ots.treas.gov>. In addition, you may inspect comments at the Public Reading Room, 1700 G Street, NW., by appointment. To make an appointment for access, you may call (202) 906-5922, send an e-mail to public.info@ots.treas.gov, or send a facsimile transmission to (202) 906-7555. (Please identify the materials you would like to inspect to assist us in serving you.) We schedule appointments on business days between 10 a.m. and 4 p.m. In most cases, appointments will be available the business day after the date we receive a request.

FOR FURTHER INFORMATION CONTACT:

OCC: Aida Plaza Carter, Director, Bank Information Technology Operations Division, (202) 874-4740; Clifford A. Wilke, Director, Bank Technology Division, (202) 874-5920; Amy Friend, Assistant Chief Counsel, (202) 874-5200; or Deborah Katz, Senior Attorney, Legislative and Regulatory Activities Division, (202) 874-5090.

Board: Donna L. Parker, Supervisory Financial Analyst, Division of Banking Supervision & Regulation, (202) 452-2614; Thomas E. Scanlon, Counsel, Legal Division, (202) 452-3594; or Joshua H. Kaplan, Attorney, Legal Division, (202) 452-2249.

FDIC: Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898-3872; Patricia I. Cashman, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898-6534; or Robert A. Patrick, Counsel, Legal Division, (202) 898-3757.

OTS: Robert Engebret, Director, Technology Risk Management, (202) 906-5631; Lewis C. Angel, Senior Project Manager, Technology Risk Management, (202) 906-5645; Elizabeth Baltierra, Program Analyst (Compliance), Compliance Policy, (202) 906-6540; or Paul Robin, Special Counsel, Regulations and Legislation Division, (202) 906-6648.

SUPPLEMENTARY INFORMATION:

I. Background

The Agencies have published Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Security Guidelines").² These Security Guidelines were published to fulfill a requirement in section 501(b) of the Gramm-Leach-Bliley Act in which Congress directed the Agencies to establish standards for

financial institutions relating to administrative, technical, and physical safeguards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.³

Among other things, the Security Guidelines direct financial institutions to: (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3) assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.⁴

This proposed Guidance, published as an Appendix to this notice, interprets section 501(b) of the Gramm-Leach-Bliley Act and the provisions of the Security Guidelines noted above.⁵ It describes the Agencies' expectations that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of customer information maintained by the financial institution or its service provider. The proposed Guidance further describes the components of a response program, which includes procedures for notifying customers about incidents of unauthorized access to customer information that could result in substantial harm or inconvenience to the customer. The proposed Guidance provides that a financial institution is expected to expeditiously implement its response program to address incidents of unauthorized access to or use of customer information. A response program should contain policies and procedures that enable the financial institution to:

A. Assess the situation to determine the nature and scope of the incident, and identify the information systems and types of customer information affected;

B. Notify the institution's primary Federal regulator and, in accordance with applicable regulations and

guidance, file a Suspicious Activity Report and notify appropriate law enforcement agencies;

C. Take measures to contain and control the incident to prevent further unauthorized access to or use of customer information, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls; and

D. Address and mitigate harm to individual customers.

The proposed Guidance describes the following corrective measures a financial institution should include as a part of its response program in order to effectively address and mitigate harm to individual customers:

A. Flag Accounts—The institution should identify accounts of customers whose information may have been compromised, monitor those accounts for unusual activity, and initiate appropriate controls to prevent the unauthorized withdrawal or transfer of funds from customer accounts.

B. Secure Accounts—The institution should secure all accounts associated with the customer information that has been the subject of unauthorized access or use.

C. Customer Notice and Assistance—The institution should, under certain circumstances, notify affected customers when *sensitive customer information* about them is the subject of unauthorized access. Where the institution can specifically identify affected customers from its logs, notification may be limited to those persons only. Otherwise, the institution should notify each customer in those groups likely to be affected.

The proposed Guidance provides that a financial institution should notify each affected customer when 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. For the purposes of the proposed Guidance, the Agencies define *sensitive customer information* to mean a customer's social security number, personal identification number (PIN), password, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. *Sensitive customer information* would also include any combination of components of customer information

² 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D-2, and part 225, app. F (Board); 12 CFR part 364, app. B (FDIC); and 12 CFR part 570, app. B (OTS).

³ 15 U.S.C. 6805(b).

⁴ Security Guidelines, Paragraph III.B.2.

⁵ The Agencies may treat an institution's failure to implement final Guidance issued as a violation of the Security Guidelines.