

program.¹⁰ Having such a program in place will allow the institution to quickly respond¹¹ to incidents involving the unauthorized access to or use of customer information in its own customer information systems that could result in substantial harm or inconvenience to a customer. Under the Guidelines, an institution's customer information systems consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers.¹²

Timely notification of customers, under the circumstances described below, is important to manage an institution's reputation risk. Effective notice may reduce legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft.

A response program should contain the following components:

A. Assess the Situation.

The institution should assess the nature and scope of the incident, and identify what customer information systems and types of customer information have been accessed or misused.

B. Notify Regulatory and Law Enforcement Agencies

The institution should promptly notify its primary Federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers.

An institution also should file a Suspicious Activity Report ("SAR"), if required, in accordance with the applicable SAR regulations¹³ and Agency guidance.¹⁴

¹⁰ See FFIEC Information Security Booklet, Dec. 2002; Federal Reserve SR 97-32, Sound Practice Guidance for Information Security for Networks, Dec. 4, 1997; OCC Bulletin 2000-14, "Infrastructure Threats—Intrusion Risks" (May 15, 2000); OTS CEO Memorandum 109, Transactional Web Sites, June 10, 1999; CEO Memorandum 70, Statement on On-Line Personal Computer Banking, June 23, 1997; CEO Memorandum 59, Risk Management of Client/Server Systems, Oct. 24, 1996, for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

¹¹ Financial institutions are expected to provide employees with the training necessary to understand their roles and responsibilities in order to expeditiously implement the institution's response program to address incidents of unauthorized access to and use of customer information.

¹² See Security Guidelines Paragraph I.C.f.

¹³ 12 CFR 21.11 (national banks, federal branches and agencies); 12 CFR 208.62 (state member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured state branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (state non-member banks); and 12 CFR part 563 (savings associations).

¹⁴ National banks must file SARs in connection with computer intrusions and other computer crimes. See OCC Bulletin 2000-14, "Infrastructure Threats—Intrusion Risks" (May 15, 2000); Advisory Letter 97-9, "Reporting Computer Related Crimes" (November 19, 1997) (general guidance still applicable though instructions for new SAR form

Consistent with the Agencies' SAR regulations, in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, the institution should immediately notify, by telephone, appropriate law enforcement authorities and its primary regulator, in addition to filing a timely SAR.

C. Contain and Control the Situation

The financial institution should take measures to contain and control the incident to prevent further unauthorized access to or use of customer information, while preserving records and other evidence.¹⁵ Depending upon the particular facts and circumstances of the incident, these measures could include, in connection with computer intrusions: (i) Shutting down applications or third party connections; (ii) reconfiguring firewalls in cases of unauthorized electronic intrusion; (iii) ensuring that all known vulnerabilities in the financial institution's computer systems have been addressed; (iv) changing computer access codes; (v) modifying physical access controls; and (vi) placing additional controls on service provider arrangements.

D. Corrective Measures

Once an institution understands the scope of the incident and has taken steps to contain and control the situation, it should take measures to address and mitigate the harm to individual customers. For example, the institution should take the following measures:

1. Flag Accounts

The institution should immediately begin identifying and monitoring the accounts of those customers whose information may have been accessed or misused. In particular, the institution should provide staff with instructions regarding the recording and reporting of any unusual activity, and if indicated given the facts of a particular incident, implement controls to prevent the unauthorized withdrawal or transfer of funds from customer accounts.

2. Secure Accounts

When a checking, savings, or other deposit account number, debit or credit card account number, personal identification number (PIN), password, or other unique identifier has been accessed or misused, the financial institution should secure the account, and all other accounts and bank services that can be accessed using the same account number or name and password combination until such time as the financial institution and the customer agree on a course of action.¹⁶

published in 65 FR 1229, 1230 (January 7, 2000)). See also Federal Reserve SR 01-11, Identity Theft and Pretext Calling, Apr. 26, 2001; SR 97-28, Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions, Nov. 6, 1997; FDIC FIL 48-2000, Suspicious Activity Reports, July 14, 2000; FIL 47-97, Preparation of Suspicious Activity Reports, May 6, 1997; OTS CEO Memorandum 139, Identity Theft and Pretext Calling, May 4, 2001; CEO Memorandum 126, New Suspicious Activity Report Form, July 5, 2000.

¹⁵ See FFIEC Information Security Booklet, Dec. 2002, pp. 68-74.

¹⁶ The institution should also consider the use of new account numbers and steps to ensure that

3. Customer Notice and Assistance

Under the Security Guidelines, financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. An institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so. Under the circumstances described in Paragraph III., the institution should notify and offer assistance to customers whose information was the subject of the incident.¹⁷ If the institution is able to determine from its logs or other data precisely which customers' information was accessed or misused, it may restrict its notification to those individuals. However, if the institution cannot identify precisely which customers are affected, it should notify each customer in groups likely to have been affected, such as each customer whose information is stored in the group of files in question.

a. Delivery of Customer Notice—Customer notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the customer is likely to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or for those customers who conduct transactions electronically, using electronic notice.

b. Content of Customer Notice—The notice should describe the incident in general terms and the customer's information that was the subject of unauthorized access or use. It should also include a number that customers can call for further information and assistance. The notice also should remind customers of the need to remain vigilant, over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft.

Key Elements: In addition, the notice should:

- Inform affected customers that the institution will assist the customer to correct and update information in any consumer report relating to the customer, as required by the Fair Credit Reporting Act;
- Recommend that the customer notify each nationwide credit reporting agency to place a fraud alert¹⁸ in the customer's consumer reports;
- Recommend that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- Inform the customer of the right to obtain a credit report free of charge, if the customer has reason to believe that the file at the consumer reporting agency contains inaccurate information due to fraud, together with contact information regarding the nationwide credit reporting agencies; and

customers do not reuse the same or a similar personal identification number.

¹⁷ The institution should, therefore, ensure that a sufficient number of appropriately trained employees are available to answer customer inquiries and provide assistance.

¹⁸ A fraud alert will put the customer's creditors on notice that the customer may be a victim of fraud.