BUSINESS
For The Consumer www.ftc.gov
Federal Trade Commission 1-877-FTC-HELP

FTC FACTS for Business

Financial Institutions and Customer Data: Complying with the Safeguards Rule

Many financial institutions collect personal information from their customers, such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley (GLB) Act requires financial institutions to ensure the security and confidentiality of this type of information.

As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) has issued the Safeguards Rule. This Rule requires financial institutions under FTC jurisdiction to secure customer records and information.

Who Must Comply

The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers. This includes check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax prepares, courier services, and retailers that issue credit cards to consumers. The Safeguards Rule also applies to financial companies, like credit reporting agencies and ATM operators, that receive information from other financial institutions about their customers. In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

The Safeguards Rule is posted at **www.ftc.gov/privacy/glbact**. To find out whether your company is a financial institution, check section 313.3(k) of the FTC's Privacy Rule and related materials at **www.ftc.gov/privacy/glbact**.

An Added Value

Adequately securing customer information is not only the law, it makes good business sense. When you show customers that you care about the security of their personal information, you increase their level of confidence in your institution. Poorly-managed customer data can lead to identity theft. Identity theft occurs when someone steals a consumer's personal identifying information to open new charge accounts, order merchandise or borrow money.

How to Comply

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

1. designate one or more employees to coordinate the safeguards;
2. identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
3. design and implement a safeguards program, and regularly monitor and test it;
4. select appropriate service providers and contract with them to implement safeguards; and
5. evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

These requirements are designed to be flexible. Each financial institution should implement safeguards appropriate to its own circumstances. For example, some financial institutions may choose to describe their safeguards programs in a single document, while others may memorialize their plans in several different documents, such as one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may spread this responsibility among several employees who will work together.

In addition, a firm with a small staff may design and implement a more limited employee training program than a firm with a large number of employees. And a financial institution that doesn't receive or store any information online may take fewer steps to assess risks to its computers than a firm that routinely conducts business online.

Securing Information

When a firm implements safeguards, the Safeguards Rule requires it to consider all areas of its operation, including three areas that are particularly important to information security: **employee management and training**; **information systems**; and **managing system failures**. Firms should consider implementing the following practices in these areas.

Employee Management and Training

The success or failure of your information security plan depends largely on the employees who implement it. You may want to:

- Check references prior to hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
  - locking rooms and file cabinets where paper records are kept;
  - using password-activated screensavers;
  - using strong passwords (at least eight characters long);
  - changing passwords periodically, and not posting passwords near employees' computers;
  - encrypting sensitive customer information when it is transmitted electronically over networks or stored online;
  - referring calls or other requests for customer information to designated individuals who have had safeguards training; and
  - recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.
- Instruct and regularly remind all employees of your organization's policy — and the legal requirement — to keep customer information secure and confidential. You may want to provide employees with a detailed description of the kind of customer information you handle (name, address, account number, and any

other relevant information) and post reminders about their responsibility for security in areas where such information is stored — in file rooms, for example.
- Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.
- Impose disciplinary measures for any breaches.

Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on how to maintain security throughout the life cycle of customer information — that is, from data entry to data disposal:

- Store records in a secure area. Make sure only authorized employees have access to the area. For example:
  - store paper records in a room, cabinet, or other container that is locked when unattended;
  - ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
  - store electronic customer information on a secure server that is accessible only with a password — or has other security protections — and is kept in a physically-secure area;
  - don't store sensitive customer data on a machine with an Internet connection; and
  - maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area.
- Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information. Specifically:
  - if you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;
  - if you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail; and
  - if you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.
- Dispose of customer information in a secure manner. For example:
  - hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;
  - shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up;
  - erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information;
  - effectively destroy the hardware; and
  - promptly dispose of outdated customer information.
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.
- Maintain a close inventory of your computers.

Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions:

- Maintain up-to-date and appropriate programs and controls by:
  - following a written contingency plan to address any breaches of your physical, administrative or technical safeguards;

  - checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
  - using anti-virus software that updates automatically;
  - maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations; and
  - providing central management of security tools for your employees and passing along updates about any security risks or breaches.
- Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer data regularly.
- Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically.
- Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.

For More Information

Additional guidance is available at **www.ftc.gov/privacy/glbact** and **www.ftc.gov/infosecurity**. Resources at these sites may alert you to new risks to information security and help those individuals whose information may have been compromised with their next steps. In addition, the following organizations have information available to help you implement appropriate safeguards for your customer data.

- Computer Security Resource Center, The National Institute for Standards and Technology (NIST) — **www.csrc.nist.gov**
- Critical Infrastructure Assurance Office (CIAO) — **www.ciao.gov**
- Federal Deposit Insurance Corporation (FDIC) — **www.fdic.gov**
  Tools to Manage Technology Providers' Performance Risk: Service Level Agreement — **www.fdic.gov/regulations/information/btbulletins/brochure2.html**
  Effective Practices for Selecting a Service Provider — **www.fdic.gov/regulations/information/btbulletins/brochure1.html**
- National Infrastructure Protection Center (NIPC) — **www.nipc.gov**
  Seven Simple Computer Security Tips for Small Business and Home Computer Users — **www.nipc.gov/publications/nipcpub/computertips.htm**
- System Administration, Networking and Security Institute (SANS) — **www.sans.org**
  The 20 Most Critical Internet Security Vulnerabilities — **www.sans.org/top20.htm**

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and 10 Regional Fairness Boards collect comments from small business about federal enforcement actions. Each year, the Ombudsman evaluates enforcement activities and rates each agency's responsiveness to small business. To comment on FTC actions, call 1-888-734-3247.

FEDERAL TRADE COMMISSION	FOR THE CONSUMER
1-877-FTC-HELP	www.ftc.gov

September 2002