FTC FACTS for Business

Financial Institutions and Customer Information:

Complying with the Safeguards Rule

Many companies collect personal information from their customers, including 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 companies defined under the law as "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) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. But safeguarding customer information isn't just the law. It also makes good business sense. When you show customers you care about the security of their personal information, you increase their confidence in your company. The Rule is available at www.ftc.gov/privacy/privacyinitiatives/safeguards_l&r.html.

WHO MUST COMPLY?

The definition of "financial institution" includes many businesses that may not normally describe themselves that way. In fact, the Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

For more information on whether the Safeguards Rule applies to your company, consult section 313.3(k) of the GLB Privacy Rule and the Financial Activities Regulations. Both are available at www.ftc.gov/privacy/privacyinitiatives/financial_rule_l&r.html.

HOW TO COMPLY

The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company'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 company must:

✓ designate one or more employees to coordinate its information security program;

- ✓ 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;
- ✓ design and implement a safeguards program, and regularly monitor and test it;
- ✓ select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- ✓ evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. Companies should implement safeguards appropriate to their own circumstances. For example, some companies may choose to put their safeguards program in a single document, while others may put their plans in several different documents — say, 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 assign this responsibility to several employees who will work together. In addition, companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network.

SECURING INFORMATION

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: *Employee Management and Training; Information Systems;* and *Detecting and Managing System Failures*. One of the early steps companies should take is to determine what information they are collecting and storing, and whether they have a business need to do so. You can reduce the risks to customer information if you know what you have and keep only what you need.

Depending on the nature of their business operations, firms should consider implementing the following practices:

Employee Management and Training. The success of your information security plan depends largely on the employees who implement it. Consider:

- ✓ Checking references or doing background checks before hiring employees who will have access to customer information.
- ✓ Asking every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.
- ✓ Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
- ✓ Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.)
- ✓ Using password-activated screen savers to lock employee computers after a period of inactivity.
- ✓ Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.
- ✓ Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
  - Locking rooms and file cabinets where records are kept;

- Not sharing or openly posting employee passwords in work areas;
- Encrypting sensitive customer information when it is transmitted electronically via public networks;
- Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
- Reporting suspicious attempts to obtain customer information to designated personnel.

✓ Regularly reminding all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.

✓ Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.

✓ Imposing disciplinary measures for security policy violations.

✓ Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

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

✓ Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:

- Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
- Store records in a room or cabinet that is locked when unattended.
- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically-secure area.
- Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.
- Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.

✓ Take steps to ensure the secure transmission of customer information. For example:

- When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
- If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
- If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.

✓ Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule, www.ftc.gov/os/2004/11/041118disposalfrn.pdf. For example:

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
- Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.

- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

Detecting and Managing System Failures. Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:

✓ Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.

✓ Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:

- check with software vendors regularly to get and install patches that resolve software vulnerabilities;
- use anti-virus and anti-spyware software that updates automatically;
- maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations;
- regularly ensure that ports not used for your business are closed; and
- promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

✓ Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:

- keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
- use an up-to-date intrusion detection system to alert you of attacks;
- monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
- insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.

✓ Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:

- take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
- preserve and review files or programs that may reveal how the breach occurred; and
- if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.

✓ Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:

- notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
- notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
- notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm; and
- check to see if breach notification is required under applicable state law.

FOR MORE INFORMATION

Additional guidance is available at www.ftc.gov/privacy/glbact. Resources at that site may alert you to new risks to information security and give people whose information may have been compromised important first-things-first advice for responding. Visit www.onguardonline.gov for information that can help you train your employees in safe computing practices on the job and at home. In addition, the following organizations have information to help you implement appropriate safeguards for your customer data:

Computer Security Resource Center
National Institute for Standards and Technology (NIST)
www.csrc.nist.gov

National Strategy to Secure Cyberspace, Department of Homeland Security
www.dhs.gov/dhspublic/display?theme=31&content=935

The SysAdmin, Audit, Network, Security (SANS) Institute
The Twenty Most Critical Internet Security Vulnerabilities
www.sans.org/top20

United States Computer Emergency Readiness Team (US CERT)
www.us-cert.gov/resources.html

Carnegie Mellon Software Engineering Institute CERT Coordination Center
www.cert.org/other_sources

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.

Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and ten 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.

April 2006

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

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education