FTC Business Alert

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

Safeguarding Customers' Personal Information: A Requirement for Financial Institutions

Many financial institutions' transactions with customers involve the collection of personal information: 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, a federal law, requires that financial institutions take steps to ensure the security and confidentiality of this kind of customer data.

Now, as part of its implementation of the GLB Act, the Federal Trade Commission (FTC) is issuing a rule to require the financial institutions under its jurisdiction to safeguard customer records and information.

The Safeguards Rule applies to individuals or organizations that are significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers.

According to the Safeguards Rule, financial institutions must develop a **written information security plan** that describes their program to protect customer information. All programs 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 at issue. Covered financial institutions must:

- **designate the employee** or employees to coordinate the safeguards;
- **identify and assess the risks** to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- **design a safeguards program**, and detail the plans to monitor it;
- **select appropriate service providers** and require them (by contract) to implement the safeguards; and
- **evaluate the program and explain adjustments** in light of changes to its business arrangements or the results of its security tests.

Experts suggest that three areas of operation present special challenges and risks to information security: employee training and management; information systems, including network and software design, and information processing, storage, transmission and retrieval; and security management, including the prevention, detection and response to attacks, intrusions or other system failures. The Rule requires financial institutions to pay special attention to these areas.

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

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). 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.