PROSKAUER ROSE®

Client Alert

A report for clients and friends of the firm

April 2003

# FTC Safeguards Rule to Take Effect May 23, 2003

## *Covered Entities Must Have Written Information Security Program in Place*

Less than one month from now, the Federal Trade Commission's "Safeguards Rule" will take effect. The Rule requires covered entities to implement a written information security program for the handling of consumer financial data. The Safeguards Rule is authorized by the Gramm-Leach-Bliley Act, the statute that required a large number of businesses to send privacy notices to their customers beginning in 2001. All "financial institutions" regulated by the FTC that were required to send privacy notices must also comply with the Safeguards Rule by having a written information security program in place that meets the FTC's requirements.[1]

### The Gramm-Leach-Bliley Act

In 1999, Congress passed the Gramm-Leach-Bliley Act, which contained provisions governing the privacy of consumer financial information. Sections 6802 and 6803 of the Act require "financial institutions" to provide privacy policies and opt-out notices to their customers or potential customers. The FTC and other agencies adopted regulations governing such policies that took effect in July 2001. Section 6801(b) of the Act authorizes the FTC and other agencies to adopt regulations establishing "appropriate standards . . . relating to administrative, technological, and physical safeguards" to protect customer information held by "financial institutions." Section 6801(b) is the provision now being implemented by the FTC's Safeguards Rule.

One of the problems with the Gramm-Leach-Bliley Act is that the definition of "financial institutions" covered by the Act is exceedingly broad. Under the Act, a "financial institution" is any business that "significantly engage[s] in financial activities."[2] "Financial activities" is defined as including any activity that a bank can perform under the Bank Holding Company Act of 1956.[3] In recent years, the Bank Holding Company Act has been expanded to allow banks to perform more and more activities – meaning that, as a result, the Gramm-Leach-Bliley Act covers a wide variety of businesses that may not ordinarily consider themselves "financial institutions." Many such businesses unexpectedly found themselves required to send out privacy notices to their customers under Sections 6802 and 6803 in July 2001.

Congress left enforcement of the Gramm-Leach-Bliley Act to several regulatory agencies, depending on the market sector of the regulated entity. The Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Securities and Exchange Commission, and the National Credit Union Administration have already adopted regulations implementing Section 6801(b), and "financial institutions" regulated by one of those agencies must follow those regulations, not the FTC's Safeguards Rule. Similarly, insurance companies are subject to the privacy and security regulations of state insurance regulators.

The FTC's Safeguards Rule applies only to those "financial institutions" that are not regulated by one of the other agencies listed above. However, given the breadth

1 Banks, savings and loans, credit unions, broker-dealers, investment companies, investment advisers, insurance companies, and other financial institutions regulated by agencies other than the FTC must comply with the safeguards rule of the relevant agency, most of which have already taken effect. *See* 66 F.R. 8152 (Jan. 30, 2001) (NCUA Guidelines for Safeguarding Member Information); 66 F.R. 8616 (Feb. 1, 2001) (OCC, Federal Reserve, FDIC, and Office of Thrift Supervision Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness); 17 C.F.R. § 248.30 (SEC Regulation S-P provision on safeguarding information).

2 16 C.F.R. § 313.3(k)(1).

3 *See* 15 U.S.C. § 6809(3)(A); 12 U.S.C § 1843(k).

of the definition of "financial institutions," the remainder is large, and potentially includes: check-cashing businesses, financial data processors, finance companies, mortgage brokers, real estate brokers, nonbank lenders, account servicers, personal property or real estate appraisers, finder services, professional tax preparers, law firms with tax practices,[4] collection agencies, credit counselors, courier services, and retailers that issue credit cards to consumers. The Safeguards Rule also applies to companies, such as credit reporting agencies and ATM operators, that receive information from other financial institutions about their customers.

## What the Safeguard Rule Requires

The FTC's Safeguards Rule requires all "financial institutions" regulated by the FTC to adopt an information security program for safeguarding consumers' nonpublic personal information – i.e., information about individuals who have obtained financial products or services for personal, family, or home use. The program must be in writing and must contain "administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature of your activities, and the sensitivity of any customer information at issue."

The Safeguards Rule provides that an information security program must contain several elements:

1. Designated employees who are responsible for coordinating the information security program.

2. Identification of reasonably foreseeable risks to customer information that could result in unauthorized disclosure, misuse, alteration, or destruction of the information. The Commission recommends a focus on at least three types of risks: employee training and management; information systems; and prevention, detection, and response procedures.

3. Design and implementation of safeguards to protect customer information, including regular testing, monitoring, and assessment of the sufficiency of those safeguards. The safeguards may include:

   ***Employee Training & Management***

   - Checking the references of prospective employees;
   - Having employees sign confidentiality and security agreements;
   - Training employees in basic security procedures;
   - Instructing and reminding employees of the information security policy;
   - Limiting access to customer information to employees who have a business reason to access it;
   - Imposing discipline for violations of the policy.

   ***Information Systems***

   - Storing records in a secure location;
   - Providing for secure data transmission when collecting or transmitting customer information;
   - Disposing of customer information in a secure manner;
   - Using appropriate oversight or audit procedures to detect improper disclosures or theft of customer information;
   - Maintaining a close inventory of your computers.

   ***Prevention, Detection, & Response***

   - Maintaining an up-to-date written contingency plan in the event of any breaches of the safeguards;
   - Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
   - Providing for the use of anti-virus software that updates automatically;
   - Maintaining up-to-date firewalls on internet-accessible systems or networks;
   - Providing for centralized management of security tools and distribution of security updates for employees;
   - Taking steps to preserve and protect customer information in the event of a computer or other failure;
   - Maintaining systems and procedures to ensure that access to nonpublic consumer information is limited to legitimate users;
   - Notifying customers promptly of any loss, damage, or unauthorized access to their nonpublic personal information.

4. Evaluation and adjustment of the information security program in light of the results of tests, monitoring, and any other material changed circumstances since the program was devised.

5. Oversight of the protections provided by a business's service providers. As part of this oversight, regulated businesses must require their service providers to provide appropriate safeguards in their contracts with the service providers. Contracts entered into on or before June 24, 2002 would be grandfathered in, however, until May 24, 2004.

4 On behalf of the New York State Bar Association, Proskauer has filed suit against the FTC to bar application of the Gramm-Leach-Bliley regulations to law firms. *See* Compl. for Decl. Relief, *New York State Bar Ass'n v. FTC*, No. 1:02CV00810 (RBW) (D.D.C. filed Apr. 29, 2002). However, the FTC has taken the position that it has no discretion to exempt law firms from its regulations. *See* Def.'s Mot. to Dismiss, *NYSBA v. FTC* (D.D.C. filed July 1, 2002).

The Commission has stated that these requirements are designed to be flexible. So, for example, the information security program may be one document or multiple documents to account for different divisions of a company. A firm with a small staff may provide more limited employee training than a large firm with more resources. A company that conducts no business online may take fewer steps to assess risks to its computers than a firm that transacts a large proportion of its business online.

## Conclusion

One thing about the Safeguards Rule is clear: On May 23, "financial institutions" regulated by the FTC must have a written information security program in place. The Commission has in recent years stepped up its enforcement of privacy regulations, suing several companies for violations.[5] In addition, failure to comply with the Rule may have ramifications beyond an FTC enforcement action. A catastrophic security breach could potentially give rise to private claims under existing tort or securities laws, which claims might be strengthened by a failure to follow the Rule. If they have not done so already, businesses must determine quickly if they are covered by the Rule, and if so, make certain they have a policy that complies with it.

5 *See, e.g.*, *United States v. Hershey Foods Corp.*, No. 4:CV03-350 (M.D. Pa. 2003) (alleging violations of COPPA); *United States v. Mrs. Fields Famous Brands, Inc.*, No. 2:03 CV205 JTG (D. Utah 2003) (same); *In the Matter of Eli Lilly & Co.*, File No. 012 3214 (FTC 2002) (alleging deceptive trade practice in promising security of consumer information); *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS (D. Mass. 2000) (alleging deceptive trade practice in promising never to sell consumer information).



NEW YORK LOS ANGELES
WASHINGTON BOCA RATON
NEWARK PARIS

### Client Alert

**Proskauer's Computer Security Practice Group counsels clients on their obligations in the event of a computer security breach and the steps that may be taken to avoid or limit legal liability from potential computer intrusions. The following individuals serve as the contact persons and would welcome any questions you might have.**

**Christopher Wolf**
202.416.6818 — cwolf@proskauer.com

**Warren L. Dennis**
202.416.6814 — wdennis@proskauer.com

**Bruce Boyden**
202.416.6847 — bboyden@proskauer.com

Proskauer is an international law firm with more than 590 attorneys who handle a full spectrum of legal issues worldwide.