

THE EMERGING THREAT OF LEGAL LIABILITY FOR FAILURE TO PREVENT SPYWARE ATTACKS

Charles H. Kennedy¹

A number of laws and regulations require businesses to take reasonable physical, administrative and technical measures to prevent the unauthorized acquisition, alteration or destruction of valuable information -- especially personal information of consumers. These laws and regulations tend to leave the choice of specific protective measures to the discretion of affected businesses, but courts and responsible agencies will freely second-guess those decisions in the event of a data breach.

Recent legal developments have substantially increased the likelihood that a flaw in a business's information security will be discovered and enforcement action taken. Notably, California and several other states now require notification to consumers of incidents that may result in loss of consumer data.² Reports made under the terms of these laws give regulatory agencies and plaintiffs' lawyers ready access to lists of potential targets for costly and disruptive legal proceedings.

In this environment, responsible companies monitor security threats as they arise and implement new protective measures as needed. Even the most alert management, however, is hard-pressed to identify and respond to the rapid changes that technology produces. Threats that at one time seem remote may mutate rapidly into immediate, high-risk conditions that must be addressed if security incidents -- and resulting litigation -- are to be avoided.

The latest such threat is the set of software-driven intrusions referred to generically as "spyware." Until quite recently, many dismissed spyware as an annoyance for consumers rather than a threat to business networks and the valuable information they contain. Today, spyware must be viewed as a priority threat that requires a state-of-the-art response. Failure to take spyware seriously may expose an enterprise to substantial risks of adverse legal action.

This paper focuses on two laws, and two sets of implementing regulations, that undoubtedly will be used to require businesses to implement anti-spyware measures: the

¹ Charles H. Kennedy has taught cyberlaw and communications law for the past ten years at The Columbus School of Law, Catholic University of America. He is Of Counsel to Morrison & Foerster, LLP, and is an author of four books on the law of electronic communications.

² Cal. Civ. Code § 1798.82 (West 2003); *see also* Ark. SB 1167 (2005); Conn. SB 650 (2005); Del. HB 116 (2005); Fla. HB 481 (2005); Ga. SB 230 (2005); Ill. HB 1663, Public Act 094-0036 (2005); Ind. Act No. 503 (2005); La. SB 205, Act 499 (2005); Me LD 1671 (2005); Minn. H.F. 2121 (2005); Mont. HB 732 (2005); NJ A 4001/S1914 (2005); NY A4252, A3492 (2005); Nev. SB 347 (2005); NC SB 1048 (2005); ND SB 2251 (2005); RI H. 6191 (2005); Tenn. SB 2220 (2005); Tex. SB 122 (2005); Wash. SB 6043 (2005).

Gramm-Leach-Bliley Act (“GLBA”), which applies specifically to financial institutions;³ and Section 5 of the Federal Trade Commission Act, which extends GLBA-type data security obligations to all U.S. businesses.⁴

I. The Technological Threat

A. Spyware Defined

Spyware has been defined as “software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer’s consent, or asserts control over a computer without the consumer’s knowledge.”⁵ In order to understand the threat that spyware poses, it is important to move beyond this definition to understand how spyware both resembles and differs from other intrusions to which networked computers are subject.

Notably, spyware must be distinguished from unauthorized or unwanted communications that may be harmful in their own ways but do not collect information from the targeted system. Denial of service attacks, for example, do not acquire stored data but prevent authorized use of the targeted system’s resources by overloading the system with requests for data or services. Viruses, which typically arrive concealed in email attachments, Instant Messaging transmissions or P2P file sharing applications, may cause various sorts of mayhem but are not ordinarily used to gather information. Worms (which propagate without user interaction) can carry harmful payloads, such as rootkits, that create the conditions for a spyware attack, but their effects usually are confined to degrading the performance of vulnerable systems and services.⁶

True spyware uses some of the same attack vectors (*e.g.*, shared files, worms and email attachments) as other harmful transmissions, but is distinguished by its ability to collect information from a system or user and return it to the sender, or other third party, without the knowledge or consent of the user or system administrator. True spyware includes several kinds of malicious software:

³ Gramm-Leach-Bliley Financial Modernization Act, Pub. L. 106-102, 113 Stat. 1338 (1999).

⁴ Federal Trade Commission Act, 15 U.S.C. § 45(a).

⁵ Federal Trade Commission Staff Report, “Monitoring Spyware on Your PC: Spyware, Adware, and Other Software” (March, 2005) at 2 (“FTC 2005 Staff Report”).

⁶ Worms are not carried in emails, shared files or other vectors that must be opened or downloaded by users of the target systems. Instead, creators of worms identify “back door” software vulnerabilities that permit harmful code to enter the affected systems automatically. A worm’s payload may consist of nothing more than the ability to seek out and replicate itself on every vulnerable system it encounters. In one case that resulted in a prosecution, a worm reinfected the same computers repeatedly until they “crashed or became ‘catatonic.’” *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991).

- *Back Door Trojans* arrive in the guise of legitimate programs. They deploy tools, such as rootkits and remote access trapdoors, that can give a distant attacker the same control over the system as the system *administrator*. Trojans appear to be the vector of choice for installation of system monitors.
- *System Monitors* include both useful and malicious applications. Legitimate system administrators use system monitors to record and alert them to significant events on the network. Remote monitors that are downloaded surreptitiously to a network, however, can track all activity on the system and report that information to unauthorized third parties. Illicit system monitors typically arrive in Trojan horse programs downloaded by email or Instant Messaging transmissions.
- *Keyloggers* are a specific form of system monitor that acquires and records all keystrokes entered by a user or users of the targeted system. Keyloggers typically are used to acquire passwords, credit card numbers and proprietary information.
- *Adware programs* monitor Web browsing and other user activities and target advertising to the user based upon the information transmitted to the adware provider or its clients. These sometimes are installed with the user's consent, but often arrive and operate without notice or permission. Adware is spread primarily by ActiveX downloads from online advertisements or websites.⁷

B. Spyware's Growing Impact

Corporate managers may believe that spyware is primarily a problem for consumers rather than business organizations. Such a belief would not be surprising: media reporting on spyware has concentrated on the adware phenomenon, which interferes with consumers' use of the Internet from their home computers. Adware attacks, which include browser hijacking, insertion in search results of links to sites selected by an advertiser, redirection of search requests to an advertiser's website, and monitoring of online activity in order to send targeted "pop-up ads," are frustrating and costly for consumers but pose a less obvious threat to business.⁸

⁷ ActiveX is a Microsoft environment for downloading and scripting World Wide Web content. Although ActiveX makes Web downloads visually more interesting, it also is a vehicle for "drive-by" spyware downloads.

⁸ FTC 2005 Staff Report at 8-9.

Corporate America has no cause for complacency, however, about the threat that spyware poses to its systems and data. Spyware, whether used to support advertising, direct marketing or outright corporate espionage, is not the work of amateur hackers. Increasingly, spyware is a high-stakes business that will, like all businesses, follow the path of greatest profit.

The process is already well underway. In one especially lurid and well-publicized incident, several Israeli companies used Trojans hidden in emails to infiltrate the networks of competitors.⁹ Besides leading to criminal investigations and possibly causing one suicide, this spyware espionage campaign has compromised critical data of several companies and interfered with the privatization of Israel's principal telephone company.¹⁰

The Israeli saga is perhaps the most dramatic spyware incident, but other attacks have been no less serious. For example, it was reported in August, 2005 that Trojans containing keyloggers were downloaded from pornographic websites and raided accounts maintained at some fifty banks.¹¹ Similarly, in 2004, hackers installed a keylogger in the network of the Sumitomo Mitsui Bank and attempted a massive fraudulent funds transfer.¹² For every such publicized spyware attack, it must be assumed that many more have gone undetected or unreported by their victims.

In fact, in attempting to assess the dimensions of the spyware threat, it should at least be assumed that these attacks will keep pace with the overall explosion of mass data compromise events. Although the number of data breach incidents is hard to ascertain, state reporting requirements have brought events to light that otherwise might have remained unknown. Notably, the Privacy Rights Clearinghouse reports that 84 data breaches, all involving Social Security numbers or other "data elements useful to identity thieves," have been reported since February of 2005.¹³ Not all of the reported incidents involved spyware or other hacking techniques; but as spyware's sophistication and availability improve, we can expect its use as a means of stealing valuable data to increase.

C. Defending against Spyware

In order to protect networks and information from the spyware threat, system administrators and users must take reasonable measures to reduce three categories of risk:

⁹ See "Trojan Spyware Suspects Arrested," National Infrastructure Security Coordination Centre ("NISSC") Monthly Bulletin (June, 2005).

¹⁰ "Key Suspect in 'Trojan Horse' Hacking Scandal in Apparent Suicide Bid," Agence France Presse (June 8, 2005).

¹¹ NISSC Monthly Bulletin (August, 2005).

¹² *Id.*, March/April 2005.

¹³ Privacy Rights Clearinghouse, "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

(a) the harmful transmissions and downloads that carry spyware programs; (b) the software vulnerabilities that facilitate spyware infection; and (c) the spyware programs themselves.

Protective actions of the *first kind* -- that is, avoidance of harmful downloads -- include both administrative and technical measures.

On the administrative side, organizations must establish and enforce Internet usage policies. All employees should be cautioned against opening email attachments from unknown sources, downloading shareware from the Web, clicking on ads they find on the Internet, or engaging in peer-to-peer file sharing at their workstations. Those policies must be reinforced by training and backed up by disciplinary action where appropriate.

On the technical side, system administrators should consider disabling ActiveX and other scripting technologies that are used for “drive-by” spyware insertions, and should configure firewalls to block transmissions from sites that already are identified as sources of spyware.

Protective actions of the *second kind* -- that is, correction of known software vulnerabilities-- might include replacement of browsers that are known to be especially susceptible to security holes. In any case, system administrators should install and activate vendors’ security patches as soon as they are made available.

Finally, the *third line of defense* against spyware is the use of products that identify, remove or prevent installation of all known variants of malicious spyware code. Employee training, firewall settings and security patch installations are no substitute for this third step. Not all spyware downloads require careless actions -- or any actions -- by users; security patches address only those vulnerabilities that already have been discovered and may already have been exploited; and firewalls do not detect harmful code that is carried surreptitiously in transmissions from “trusted” sites. Only products that identify and block harmful payloads hidden within transmissions that would not otherwise be blocked offer a robust defense against spyware.

Users and administrators also should know that not all anti-spyware products are equal. Anti-virus products may not address spyware, or may do so only incompletely. Even some specialized anti-spyware products use approaches, such as compilation of spyware definitions based upon visits to known spyware sites or reports from clients that do not identify all existing threats or do so only after machines have been infected.

The most effective form of spyware protection, in fact, is a product of the “Web crawler” variety that dynamically seeks out and identifies new forms of spyware as they appear. These approaches are best calculated to stay ahead of the threat curve rather than play a constant game of “catch up.”

II. THE LEGAL THREAT

If your enterprise is attacked by spyware, you are not just a victim: you also are a potential defendant. Today's legal environment makes businesses responsible for failing to prevent foreseeable attacks, including spyware attacks, that result in harm to consumers.

Many enterprises still are unaware of the extent of their exposure for data breaches. Until recent years, government agencies let businesses decide for themselves how they would deal with information security risks. With few exceptions, such as those applicable to bank information systems, no statute or regulation required private businesses to conduct security training, make threat assessments, encrypt data, transmit information over virtual private networks or other secure lines, assign user names and passwords, or take other protective measures. By avoiding interference with these decisions, government allowed data protection technologies to evolve without regulatory distortion and left businesses free to provide as much or as little data protection as their customers wanted and were willing to buy.

The legal environment has changed, however, in three important ways. First, Congress has passed privacy legislation that subjects specific industries to data protection obligations for personal information they collect and maintain. Second, the Federal Trade Commission ("FTC") and some states have used their consumer protection authority to extend data protection obligations to American business more generally -- not by writing new rules, but by bringing enforcement actions against individual companies. Third, the plaintiffs' bar has discovered data security and has begun to bring class action suits against companies that lose consumers' personal information. These public and private enforcement initiatives are likely to continue, and will affect companies that are not subject to specific data protection statutes and may believe, incorrectly, that they still are free to use business judgment in their choice of data protection measures.

Perhaps the most comprehensive information security obligations are those imposed on financial institutions by the Gramm Leach Bliley Act and the implementing regulations of the various oversight agencies that regulate those institutions. The GLBA, which reinforces a substantial legacy of banking data security regulations, has made U.S. financial institutions some of the most security-conscious businesses in the world.

The most important single enforcer of data protection standards, and the agency that sets the pace for other federal and state initiatives in this area, is the Federal Trade Commission. Beginning at least 10 years ago, when it held a series of hearings on the privacy of information submitted to Internet sites, the FTC has made privacy and data security an enforcement priority under its authority, granted in Section 5 of its enabling statute, to regulate unfair or deceptive acts and practices. The intervening years have only increased the Commission's aggressiveness as a creator and enforcer of privacy rights.

The following takes the GLBA obligations, and those adopted by the FTC under Section 5, in turn.

A. The Data Security Regime of the Gramm Leach Bliley Act

The GLBA is best known to the public for its restrictions on disclosure by financial institutions of nonpublic personal information to third parties, but the statute also requires various federal and state agencies to set standards for the administrative, technical, and physical protection of the customer records and information of financial institutions. Pursuant to this requirement, the Office of the Comptroller of the Currency (“OCC”), the Federal Reserve Board (“FRB”), the Federal Deposit Insurance Corporation (“FDIC”), the Office of Thrift Supervision (“OTS”), and the FTC all have promulgated regulations that govern the data protection practices of institutions and activities within their jurisdictions. State authorities also have enacted GLBA security rules applicable to insurance companies.

The banking industry’s principal GLBA data security regulations are the “Interagency Guidelines Establishing Standards for Safeguarding Customer Information” adopted jointly by the OCC, OTS, FRB and FDIC and published on February 1, 2001 (“Interagency Guidelines”).¹⁴ The Interagency Guidelines set out the elements of a rigorous data security regime that all covered financial institutions must establish and maintain. In order to comply with these requirements, each covered financial institution must “implement a comprehensive written information security program . . . [that is] designed to: (1) Ensure the accuracy and confidentiality of customer information; (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.”¹⁵ This program must be developed and implemented with the involvement of the institution’s Board of Directors, and must be based upon a risk assessment that identifies “reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.”¹⁶ Based upon this risk assessment, each institution must implement a program that includes, as appropriate, “[m]onitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems,” and response programs that “specify actions to take when you suspect or detect that unauthorized individuals have gained access to customer information systems”¹⁷

¹⁴ Department of the Treasury, Office of the Comptroller of the Currency, 12 CFR Part 30 [Docket No. 00-35], RIN 1557-AB84; Federal Reserve System, 12 CFR Parts 208, 211, 225, and 263 [Docket No. R-1073]; Federal Deposit Insurance Corporation, 12 CFR Parts 308 and 364, RIN 3064-AC39; Office of Thrift Supervision, 12 CFR Parts 568 and 570 [Docket No. 2000-112], RIN 1550-AB36.

¹⁵ *See, e.g.*, 12 CFR Part 570 Appendix B, § II(B).

¹⁶ *Id.* § III(B).

¹⁷ *Id.* § III(C)(1)(f)-(g).

Each institution's information security program, including all "key controls, systems and procedures," must be periodically tested, reassessed and updated as appropriate. Tests of the program's controls, systems and procedures must be "conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."¹⁸ Each institution must report to its board, or an appropriate committee of its board, at least annually the "status of the information security program" and the company's compliance with the Guidelines.¹⁹

Each regulatory agency has the authority to examine financial institutions under its jurisdiction for compliance and can determine that those institutions have failed to satisfy the requirements of the Guidelines; and the OCC, FRB and FDIC may characterize such failures as violations, not only of banking regulations, but of the prohibition against unfair and deceptive acts or practices set out in the FTC Act.²⁰

Violations can result in payment of substantial penalties and restitution to affected customers. Although penalties specifically related to the Guidelines appear not to have been imposed so far, the magnitude of past penalties for unfair and deceptive practices by financial institutions gives some idea of the potential scale of liability. For example, in a case involving Provident National Bank, the institution was required to pay \$300 million in restitution to customers for abuses related to guaranteed savings rate, credit protection and other programs.²¹ Similarly, in a case involving the First National Bank of Marin, the bank was ordered to establish a reserve to handle restitution payments, with an initial deposit to that fund of \$4 million.²² Other, recent investigations have resulted in restitution by Direct Merchants Credit Card Bank, First Consumers National Bank, and the First National Bank in Brookings.²³

¹⁸ *Id.* § III(C)(3).

¹⁹ *See id.* § III(F).

²⁰ *See, e.g.*, 12 CFR § 308.302(a). Banking regulators take the position that they may, under section 8 of the Federal Deposit Insurance Act, "enforce section 5 of the FTC Act when a bank subject to their supervision has engaged in an unfair or deceptive act or practice – whether or not there is [a banking] regulation defining the particular act or practice as unfair or deceptive." J. Williams and M. Bylsma, "On the Same Page: Federal Banking Agency Enforcement of the FTC Act to Address Unfair and Deceptive Practices by Banks," 58 Bus. Law. 1243 (May, 2003). As discussed below, the FTC takes the position that data security failures may constitute unfair or deceptive practices, and banking regulators likely will follow that guidance in their own efforts to enforce the FTC Act against regulated financial institutions.

²¹ Press Release, OCC, "Provident to Cease Unfair Practices, Pay Consumers Minimum of \$300 Million Under Settlement with OCC and San Francisco District Attorney (June 28, 200), <http://www.occ.treas.gov/ftp/release/2000-49.doc>.

²² *See* Federal Document Clearinghouse Congressional Testimony, J. Williams, Acting Comptroller of the Currency, before the Senate Banking, Housing and Urban Affairs Committee (May 17, 2005).

²³ *Id.*

Bank regulators now are making data security a particular focus of their examinations of institutions under their jurisdiction, and protection against spyware has been specifically identified as an enforcement issue. Notably, the Federal Deposit Insurance Corporation issued guidelines on July 22, 2005 that warn of the potential use of spyware to commit identity theft. The FDIC urged its member institutions to educate consumers about the spyware threat and “stay vigilant about the risks involved with this malicious software.”²⁴

In light of the spyware-related attacks on Sumitomo Mitsui and other banks described above, failure to protect adequately against spyware intrusions likely will result in aggressive enforcement action by bank regulators.

B. Data Security under Section 5 of the FTC Act

The FTC’s concern with data security, as distinguished from privacy generally, dates at least from its adoption of regulations to enforce the GLBA.²⁵ The FTC’s so-called “Safeguards Rule,” which since has become the template for all FTC enforcement actions involving data security, was proposed in September, 2000 and took effect on May 23, 2003.

The FTC Safeguards Rule directs all entities covered by the GLBA to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.”²⁶ The Safeguards Rule sets out a number of steps that covered entities must take in developing, implementing and maintaining such a program,²⁷ including:

1. designation of an employee or employees to coordinate the program;
2. a comprehensive assessment of internal and external threats to information security, including those related to employee training and management, network and software design, and intrusion detection, prevention and response capabilities;²⁸ and

²⁴ FDIC Financial Institution Letters, FIL-66-2005, “Guidance on Mitigating Risks from Spyware” (July 12, 2005), <http://www.fdic.gov/news/news/financial/2005/fil6605.html>.

²⁵ 16 C.F.R. Pt. 314 (2002). See Appendix A.

²⁶ 16 C.F.R. Pt. 314, § 314.3(a)(2002).

²⁷ *Id.* § 314.4(a).

²⁸ *Id.* § 314.4(b).

3. design and implementation of “information safeguards to control the risks you identify through risk assessment,” including testing and monitoring of the effectiveness of the methods adopted.²⁹

The Rule also requires covered entities to oversee the information security practices of contractors and conduct periodic reassessments and modifications of information security procedures.³⁰

The FTC’s Safeguards Rule has had an impact well beyond the financial institutions to which it explicitly applies. Because the FTC has a broad consumer-protection mandate that applies to businesses generally, the FTC has the means to turn its Safeguards Rule into a *de facto* standard for most of the U.S. economy. All that is required is to attack failures to implement GLBA-type measures as “unfair or deceptive acts or practices,” which already are prohibited by Section 5 of the FTC Act.³¹ The FTC has taken advantage of this jurisdiction, first by attacking data protection failures as “deceptive” and more recently by attacking those failures as “unfair.”

The FTC’s data security enforcement actions under Section 5 have involved a wide range of American industries and lines of business, from software (Microsoft) to pharmaceuticals (Eli Lilly) to entertainment (Tower Records).³² In these and other proceedings, the Commission has used data security breaches or defects as a basis for imposition of the entire range of Safeguards Rule obligations, in the form of consent decrees that subject the target companies to FTC oversight for 20 years. Similar actions have been brought by state governments, often acting under the authority of those states’ own “Little FTC Acts;” and all of those proceedings are closely watched by the plaintiff’s bar, which has begun to bring class action lawsuits based upon mass data losses.³³

²⁹ *Id.* § 314.4(c).

³⁰ *Id.* §§ 314.4(d), 314.4(e).

³¹ 15 U.S.C. § 45(a).

³² *See, e.g., Eli Lilly and Co.*, Docket No. C-4047 (May 8, 2002), <http://www.ftc.gov/opa/2002/01/elililly.htm>; *In the Matter of Microsoft Corp.*, File No. 012-3240, <http://www.ftc.gov/spa/2002/08/microsoft.htm>; *In the Matter of GUESS?, INC., a corporation, and GUESS.COM, INC., a corporation*, File No. 022-3260, <http://www.ftc.gov/os/2003/06/guesscmp.htm>; *In the Matter of MTS, Inc., doing business as Tower Records/Books/Video, a corporation and Tower Direct, LLC doing business as Tower Records.com, a corporation*, File No. 032-3209, <http://www.ftc.gov/os/caselist/0323209.htm>.

³³ *See, e.g., In the Matter of Ziff Davis Media Inc., Assurance of Discontinuance* effective Aug. 28, 2002, Office of New York State Attorney General, www.oag.ny.us (“Ziff Davis Assurance of Discontinuance”); *State of Ohio v. DSW, Inc.*, Case No. 05CV06-6128 (Complaint for Declaratory Judgment, Court of Common Pleas, Franklin County, Ohio, June 6, 2005), Press Release of Attorney General Jim Petro at http://www.ag.state.oh.us/press_releases/2005/pr20050606.htm.

The history of enforcement proceedings under Section 5 of the FTC Act holds many lessons for companies that are affected, or may be affected, by spyware. Those lessons include the following:

1. Spyware Is An Emerging FTC Enforcement Priority

The FTC's history as a privacy enforcer follows a familiar pattern. First the FTC holds hearings, writes reports or otherwise broadcasts its interest in a privacy-related subject. Concurrently with or soon after the initiation of those efforts, the FTC brings enforcement actions against companies that fail to address the FTC's concerns in a way the Commission thinks appropriate.

For example, the Commission held hearings, beginning in the mid-1990s, concerning online collection of personal information and issued reports on that subject in 1998, 1999 and 2000.³⁴ The Commission at first supported industry self-regulation as the preferred method of protecting online privacy, but in its 2000 Report urged the Congress to pass comprehensive online privacy legislation. Even in the absence of such legislation, the FTC used its Section 5 authority against companies that failed to protect the privacy of information submitted online.³⁵

Similarly, in 2002, the Commission opened a data security initiative, including its "Dewie the Turtle" public education campaign.³⁶ That same year saw the FTC's enforcement action against Eli Lilly, which proved to be the first of a series of actions against companies that allegedly had failed to protect personal information stored on their networks.

The FTC appears to be following a similar approach in the area of spyware protection. In April 2004, the Commission held a workshop on the subject of spyware.³⁷ In further support of its inquiry, the Commission requested and received a report on spyware from its staff and issued a report on the subject to Congress.³⁸ As should be expected, the

³⁴ See Federal Trade Commission, "Privacy Online: A Report to Congress" (June 1998); "Self-Regulation and Privacy Online" (July 1999); "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress" (May 2000); available at <http://ftc.gov>.

³⁵ See *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000); *Liberty Financial Companies, Inc.*, FTC Docket No. C-3891 (Aug. 12, 1999); *GeoCities*, FTC Docket No. C-3849 (Feb. 12, 1999).

³⁶ See FTC News Release, "FTC Introduces Internet Safety Mascot, 'Dewie the Turtle,' at Privacy 2002 Conference" (Sep. 26, 2002), <http://ftc.gov.opa/2002/09/dewie.htm>.

³⁷ "Workshop, "Monitoring Software on Your PC: Spyware, Adware, and Other Software" (April 19, 2004), announcement, transcript and other materials available at <http://ftc.gov/bcp/workshops/spyware/index.htm>.

³⁸ Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science & Transportation Subcommittee on Trade, Tourism, and Economic Development, United States Senate (October 5, 2005); FTC Staff Report, "Monitoring Software on Your PC" (March, 2005), <http://www.ftc.gov>.

FTC also has undertaken its first stage of enforcement proceedings against spyware providers and advertisers of false anti-spyware products.³⁹

If the FTC stays true to form, we can expect its litigation efforts to turn to companies that did not create or knowingly facilitate spyware, but failed to protect consumer data adequately against the spyware threat. The FTC's past enforcement history gives us ample notice of the kinds of charges that will be brought in these proceedings.

2. Failures to Prevent Spyware Intrusions Will Be Attacked as Unfair and Deceptive

The FTC's enforcement actions against companies that fail to defend against spyware is likely to take two forms.

First, the Commission will look for spyware-related violations of public statements, made in privacy policies, advertising or elsewhere, that commit companies to protect consumers' data. Those commitments need not mention spyware; in fact, they might not refer to any specific security measures at all. Nonetheless, the FTC will construe those statements as commitments to implement the full range of protections called for by the Safeguards Rule. Accordingly, if a company suffers a security incident because of failure to include spyware protection in its security plan, the FTC will claim that the company's privacy assurances were deceptive. Unless the target company resists the FTC's action in a costly and embarrassing judicial proceeding, the usual 20-year consent decree will follow, perhaps supplemented by substantial fines.⁴⁰

Second, the FTC will look for companies that may have said nothing to the public about their data security practices, but that nevertheless have failed to protect against spyware with a level of vigilance acceptable to the Commission. As the FTC's recent action against BJ's Wholesale Club shows, failures to protect networks against intrusions that

³⁹ For a summary of the FTC's enforcement efforts as of October, 2005, see Federal Document Clearing House Congressional Testimony, D. Majoras, Chairman, Federal Trade Commission before Subcommittee of Trade, Tourism and Economic Development of Senate Commerce, Science and Transportation Committee (Oct 5, 2005). State law enforcement officials also are moving aggressively against vendors of spyware. See BNA Privacy Law Watch, "Internet Firm Leader to Pay \$750,000 in Settlement of Spitzer Adware Probe" (Oct. 21, 2005).

⁴⁰ This is the pattern followed in the Commission's "deception" actions against companies that allegedly failed to implement promised data security measures. In at least two of those cases (Eli Lilly and Tower) the security assurances given by the respondent companies were highly general and were not clearly inconsistent with the practices those companies actually employed. The supposed inconsistency between these statements and the respondents' practices, however, was sufficient for the Commission to demand 20-year consent decrees from those companies.

compromise customer data are considered unfair and will be attacked regardless of the security commitments the targeted company may or may not have made.⁴¹

The FTC will scour the country for appropriate targets of this campaign. In its post enforcement actions, the FTC has not confined itself to companies that suffered actual data losses. Tips about security practices from disgruntled employees and “white hat” hackers, or investigations undertaken on the Commission’s own initiative, are sufficient to begin the process. Specific charges might include the following:

a. Failure to Include Spyware in the Enterprise’s Risk Assessment

According to the Commission’s Safeguards Rule, the foundation of every security program is a written risk assessment that examines all “reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information,” and that assesses “the sufficiency of any safeguards in place to control those risks.”⁴² The risk assessment must be comprehensive and must include, among other threats, “attacks, intrusions, or other systems failures.”⁴³

A risk assessment that will pass muster with the FTC is a complex process. The project can usefully be divided into four stages. In the *asset valuation and classification* stage, the company identifies its principal information assets and categorizes them according to their value, defined as the impact on the company if those assets are destroyed, altered or disclosed without authorization. (Unauthorized destruction, alteration and disclosure may be referred to collectively as *adverse events*.) Depending upon their classifications in this process, a company’s information assets will receive different levels of protection in the eventual data security plan. In the *risk identification* stage, the company identifies the personnel-based, facilities-based and information system-based vulnerabilities that might increase the likelihood of adverse events. In the *data security evaluation* stage, the company compares its present data security measures to the best-practice measures that U.S. corporations generally use to control vulnerabilities of the kinds identified in the risk identification stage, and identifies any data security shortfalls that must be corrected. Finally, in the *risk management* stage, the company adopts and implements a data security plan,

⁴¹ According to the FTC, BJ’s had committed unfair acts and practices when it failed to implement reasonable procedures to protect its customers’ credit and debit card information. BJ’s apparently had transmitted and stored this information in unencrypted form, using computer networks that could be accessed by means of default passwords and insecure wireless connections, with the result that several millions of dollars were fraudulently charged to customers’ accounts. BJ’s has not admitted wrongdoing, but the parties have agreed to a consent decree that will subject BJ’s to federal oversight of its information security practices for the next twenty years. *In the Matter of BJ’s Wholesale Club*, Docket No. C-4148, Decision and Order (Sept. 23, 2005).

⁴² Safeguards Rule § 314.4(b).

⁴³ *Id.*

including the written policies, training programs and technical measures that are needed to carry out that plan.⁴⁴

A miscalculation at any stage of this process can result in the adoption of inadequate policies and practices. Where spyware is concerned, the risk assessment must accurately identify the information assets that spyware can affect and the value of those assets to the company. (As noted earlier, it should not be assumed that spyware intrusions, like viruses, will only affect system performance and will not steal or corrupt information assets.) Similarly, the risk identification stage of the assessment must accurately reflect the likelihood of spyware attacks and the magnitude of the loss to the company – financial, reputational and legal – if those attacks succeed. If the asset valuation and classification and risk identification judgments are incorrect, the company’s assessment of its current practices and the resulting data security plan will be flawed. As a legal matter, this will have two effects: first, the FTC will find the data security plan defective under the Safeguards Rule; second, the defective risk assessment will, itself, form an independent basis of liability under the Rule.

Finally, companies that have only recently become aware of the spyware threat should immediately update their risk assessments and refine their security plans accordingly. The Safeguards Rule requires period reassessment of each company’s security plan, and a risk assessment and plan that does not take new spyware technologies into account will very likely understate the risk from “attacks, intrusions, and other systems failures.”

b. Failure to Include Spyware in the Written Security Plan

FTC investigations into data security practices typically begin with requests to review the target companies’ security plans and implementing documents, which are required by the Safeguards Rule to be “written in one or more readily accessible parts” and must include “administrative, technical, and physical safeguards that are appropriate to [the company’s] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.”

If your company is accused of inadequate anti-spyware measures, your defense will be aided if the written plan you submit to the Commission specifically addresses spyware and sets out the administrative, technical, and physical measures you have undertaken to reduce that threat and its impact. Put more bluntly, failure to provide the Commission with such a written plan, even if you have in fact taken adequate anti-spyware measures, will prolong the investigation and increase the likelihood of a negative outcome. As anyone who has been

⁴⁴ Risk assessment and security policy templates are set out in a number of “best practice” documents from private and governmental sources. *See, e.g.*, Carnegie Mellon Software Institute Handbook for Security Incident Response Teams (“CSIRT”). None of those templates, however, is a “one size fits all” procedure that can be applied to a specific company without modification. *See also* R. Peltier, *Information Security Risk Analysis* (CRC Press 2001).

involved in one of these inquiries will attest, the FTC is highly skeptical of claims to have taken protective measures that are not fully documented.

c. Failure to Develop and Implement Appropriate Administrative Measures

Companies typically think of hacking and other technical intrusions as threats that require IT solutions, but the administrative side of attack-proofing a network can be as important as encryption, firewalls, and anti-spyware technologies.

Notably, spyware often relies upon social engineering techniques (for example, inducing an employee to open an email attachment that launches an attack) and other methods that exploit the absence of clear Internet usage policies and employee training. As in the Eli Lilly case, in which an employee accidentally sent an email to users of Prozac that disclosed all addresses on the listserv, the FTC will seize upon any misstep by your personnel as evidence that proper procedures and training were not developed and implemented. Accordingly, you should ensure, not only that you communicated proper practices to your personnel, but that you can document those communications.

d. Failure to Implement Technical Anti-Spyware Measures

The Safeguards Rule requires companies to adopt technical measures that are appropriate to the data security risks it has identified, including the risk of “attacks, intrusions, or other systems failures.” Although the Safeguards Rule does not specify the kinds of technical measures that will be considered appropriate in any particular case, companies can count on the FTC to assume that if an intrusion occurs and could have been prevented by an available technology, the decision not to use that technology was defective. This will be so, even if a complex and expensive risk assessment concluded that the magnitude of risk did not justify the cost of deploying the protective technology.

In its recent action against Columbia House for violation of the Do Not Call Rule, for example, the FTC noted tersely that the company adopted technical measures to screen telephone numbers that could not lawfully be called, but that those measures were ineffective. Similarly, in the recent BJ’s case, the Commission specifically pointed out that sensitive in-store communications and stored data were not encrypted. The FTC appears not to have engaged in any cost-benefit analysis of alternative technical measures in these cases, and companies embroiled in FTC investigations should expect a simple rule to apply: if the measures you adopted did not prevent the attack and stronger measures were available, then your measures were inadequate under the Safeguards Rule.

In this unforgiving legal environment, companies should purchase and use anti-spyware products that have a strong track record and industry acceptance, and that offer the highest level of protection commercially available.

e. Failure to Comply with Industry and Regulatory Standards

Its aggressive enforcement practices notwithstanding, the FTC is not an expert agency in the area of data protection. Accordingly, The Commission will borrow liberally from industry best practices and the work of other agencies in deciding on the magnitude of the spyware threat and the type and level of response appropriate to that threat. The Commission also will look to the record made in its extensive hearings and reports on the spyware issue. Those sources offer a number of clues as to the responses that will be considered adequate.

Among other sources, the Commission is likely to take into account the standards by which corporate America is implementing its obligations under the Sarbanes-Oxley Act, including the requirement of an internal control report that acknowledges management's responsibility for establishing and maintaining adequate internal controls for financial reporting.⁴⁵ Notably, the Committee of the Sponsoring Organizations of the Treadway Commission ("COSO"), in its Control Guidance for Data Management, states under the heading of "Malicious Software, Prevention, Detection and Correction" that spyware will not be detected by firewalls or anti-virus software and "enable unauthorized access to sensitive corporate data."⁴⁶ COSO also makes the following observations:

"[A]n organization would not be in compliance with adequate controls over financial reporting if systems monitors were present on audited machines even if the company had firewalls and anti-virus deployed."⁴⁷

Similarly, COSO points out that "mobile computers need protection from these malicious spyware types, and it is critical that these PCs are free of spyware before they connect to corporate networks."⁴⁸

Similarly, the FDIC has issued guidance on spyware protection, and recommends that financial institutions consider "threats from spyware as part of the risk assessment process . . . and take[] appropriate steps to mitigate those risks, such as implementing anti-spyware technologies."⁴⁹

⁴⁵ 15 U.S.C. § 7262 (2004).

⁴⁶ COSO, Control Guidance for Data Management ("COSO Guidance"), 2.4, 5.19. COSO is a "voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance." COSO Homepage, <http://www.coso.org>.

⁴⁷ COSO Guidance § 5.19.

⁴⁸ *Id.* § 2.4.

⁴⁹ FDIC Financial Institution Letters, FIL-66-2005, "Guidance on Mitigating Risks from Spyware" (July 22, 2005), <http://www.fdic.gov/news/news/financial/2005/fil6605.html>.

Finally, the FTC's own staff report and report to Congress make clear that spyware can lead to loss of data and cannot reliably be controlled by firewalls and typical anti-virus programs. In fact, the FTC Chairman's most recent congressional testimony on this issue points out that technological solutions to spyware threats are ineffective unless they are promptly and frequently updated, and indicates that the Commission will watch technical developments in this area closely.⁵⁰ This testimony, which reflects a growing awareness at the Commission of the availability, strengths and weaknesses of technological spyware solutions, confirms the likelihood that failure to implement state-of-the-art protective technologies will attract the Commission's negative scrutiny.

III. THE SCOPE OF LIABILITY FOR SPYWARE ATTACKS

This discussion has emphasized the data protection obligations of the Gramm Leach Bliley Act and the reported civil enforcement efforts of the FTC. Companies desiring a complete understanding of the legal risk environment should be aware of two limitations of this approach.

First, the reported enforcement actions of the FTC and other agencies are only a small part of the investigatory processes ongoing at any time. Many companies are embroiled in inquiries that will never result in adverse action or become public, but that impose punishing costs on those companies in time and cost, including attorneys' fees.

Second, the FTC is the lead agency, but not the only protagonist, in the data protection legal drama. Many states are equally aggressive, and private actions – such as the class action suit recently brought against CardSystems for its massive loss of credit card data – are just beginning to become a factor.

Finally, as *The Wall Street Journal* reported in a recent online article, mass data compromise incidents have caused persistent reductions in the shareholder value of the companies involved. Fallout of this kind, even if not accompanied by investigations or lawsuits, amply justifies the attention of management to spyware and other emerging technical threats to their networks and information resources.⁵¹

⁵⁰ Congressional Quarterly, Inc., Capitol Hill Hearing Testimony, Testimony by D. Majoras, Chairman, Federal Trade Commission before Trade, Tourism, and Economic Development Subcommittee of Senate Commerce, Science and Transportation Committee (Oct. 5, 2005).

⁵¹ "Companies Pay a Price for Security Breaches," *Wall Street Journal Online* (June 15, 2005).

APPENDIX A: The FTC's Safeguards Rule

In order to comply with the Safeguards Rule, a company must “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.”⁵²

In designing and implementing such a program, a company must do the following:

- (a) Designate an employee or employees to coordinate your information security program.
- (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuses, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
 - (1) Employee training and management;
 - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
 - (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
- (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- (d) Oversee service providers, by:
 - (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

⁵² Safeguards Rule § 314.3(a).

- (2) Requiring your service providers by contract to implement and maintain such safeguards.

- (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.⁵³

⁵³ *Id.* § 314.4.