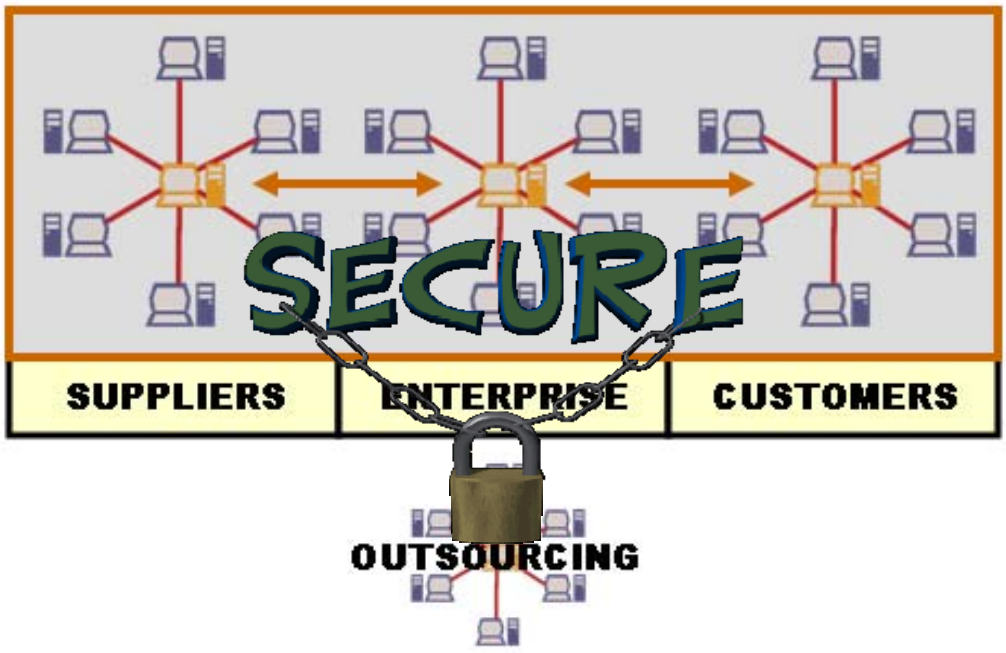
Information Security Law

An Overview

David G. Ries
Thorp Reed & Armstrong, LLP
Pittsburgh, PA
dries@thorpreed.com
(412)-394-7787

February 2007



Contents

David G. Ries

Dave Ries is a partner in the Pittsburgh office of Thorp Reed & Armstrong, LLP, where he practices in the areas of environmental, commercial and technology litigation. He has used computers in his practice since the early 1980s and chairs his firm's Technology Committee. He has represented clients in a variety of technology litigation matters and advised clients on a number of technology law issues such as hardware and software agreements, technology use policies, information security, privacy regulations, electronic records management, response to computer intrusions and electronic contracting. Dave has frequently spoken on technology law issues for legal, academic and professional groups including the American Bar Association, the Association of Corporate Counsel, the Pennsylvania Bar Institute, the Allegheny County Bar Association, Carnegie Mellon University, Duquesne University and Robert Morris University. He is a contributing author to a new American Bar Association book, *Information Security for Lawyers and Law Firms*, which was published in April 2006 and is a member of the American Bar Association Information Security Committee. Dave received his J.D. from Boston College Law School in 1974 and his B.A. from Boston College in 1971.

I. Introduction

Information security law has been a developing area of the law for a number of years—sometimes developing rapidly and at other times moving more slowly. At the same time, technology has been constantly moving at lightning pace. As a result, technology is often ahead of the law. This gap, as well as other factors, lead to substantial uncertainty in information security law. In many situations, legal requirements and remedies are unclear.

Information security requirements in the United States have usually been limited to specific segments of information, like information held by government agencies, consumer financial information, and health information. They have often been adopted in response to specific problems. Generally, legal obligations in information security and the corresponding potential for liability have been expanding.

The years 2005 and 2006 and the first 2 months of 2007 have involved unprecedented disclosures of information security breaches of consumer information, with risk of fraud and identity theft. There were over 500 reported incidents of data breaches of consumer information during these this time, exposing information concerning over 100 million records about individuals[1]. Inquiries showed that there had also been many data breaches in the past. They were often not disclosed because there were no laws which required their disclosure. A new California law, which requires disclosure of certain security breaches, was the major driver for many of the recent disclosures. Company executives testified in Congressional hearings that past security breaches were not disclosed because there were no legal requirements for breach notification. Many state legislatures have already responded with new information security laws, covering such areas as requiring reasonable security, requiring notice of breaches and providing for credit freezes. More are under consideration. At the federal level, the new Congress is considering a number of data protective laws. Bills range from national requirements for breach notification to

[1] The Privacy Rights Clearinghouse maintains a database of breaches, available at www.privacyrights.org/ar/ChronDataBreaches.htm. Attrion.org has a similar database at http://attrition.org/dataloss.

comprehensive requirements for information security. Many observers expect action this year by the new Congress. Courts have started to address the legal outfall from these breaches. Summaries of selected cases are contained in Sections III and IV of this paper.

These high profile breaches are already leading to expanded requirements and greater potential liability in the area of consumer data. They are likely to accelerate the expansion of information security obligations and potential liability in other areas of information security. It is critical for businesses and organizations of all sizes to understand the information security legal obligations which apply to them and to implement effective information security programs to address them, as well as other relevant information security considerations. In addition to legal requirements and risk of liability, there are also compelling business drivers for information security. Data breaches can lead to adverse publicity, loss of customers, and financial loss, apart from legal liability.

II. Selected Information Security Laws

A. Federal Laws

Computer Fraud and Abuse Act
18 U.S.C. § 1030 (the primary federal law which prohibits computer intrusion, damage and access beyond authorization)

- Attempts to address computer crime in a single, comprehensive statute.

- Covers a "protected computer" which is defined as a computer:

  "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
  (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States";

- Includes 7 categories of prohibited acts:

  (1) unauthorized access involving national defense, foreign relations or restricted federal government data,
  (2) unauthorized interception of covered information or communications,
  (3) unauthorized access to nonpublic federal government computers,
  (4) unauthorized access of a protected computer with the intent to commit fraud,
  (5) causing damage to protected computers,
  (6) trafficking in passwords or similar information,
  (7) extortion through a threat to damage a protected computer.

- Covers attempts to commit prohibited acts.

- Provides for criminal penalties and a private right of action for damages and equitable relief.

Electronic Communications Privacy Act
18 U.S.C. §2510-2221 (prohibits unauthorized interception and disclosure of electronic communications transmitted or stored on covered networks)

- Amendments to extend federal wiretap statutes which cover "oral" and "wire" communications by common carrier transmission.

- Extends coverage to "electronic communications" which are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate or foreign commerce," excluding "wire or oral communications," "tone only paging," a "tracking device," and stored "electronic funds transfer information" which are covered by other provisions.

- Covers interception during transmission.

- Extended by the Stored Communications Act to cover unauthorized access to electronic communications stored incident to transmission or stored for backup. 18 U.S.C. §§2701-2710.

- Provides for criminal penalties and private rights of action for damages, equitable relief, attorney fees and litigation costs.

- Provides procedures for authorized access by law enforcement.

The Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act (USA Patriot Act)
Pub. L. No. 107-56 (2001); renewed and amended in March, 2006.

- Amends several existing laws to provide the government with additional tools to track, prevent and combat terrorism.

- Provides for sharing of national security and law enforcement information.

- Provides additional government access to information, including electronic information.

- Includes amendments to the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act.

Identity Theft and Assumption Deterrence Act of 1998 – Amendments to 18 U.S.C. § 1028 (criminal sanctions for knowingly transferring or using another person's identity for unlawful purposes.)
Identity theft may also violate other federal criminal laws, like 18 U.S.C. § 1029 - credit card fraud, 18 U.S.C. § 1030 – computer fraud; 18 U.S.C. § 1341 – mail fraud; 18 U.S.C. § 1343 – wire fraud; and 18 U.S.C. § 1344 – financial institution fraud.

Identity Theft Penalty Enhancement Act of 2004 – Amendments to existing criminal statutes which establish two types of "aggravated identity theft" – identity theft in connection with terrorism and identity theft in connection with other felonies. Increases penalties and authorizes additional funding to prosecute identity theft.

Fair and Accurate Credit Transactions Act of 2003
Amendments to and reauthorization of the Fair Credit Reporting Act of 1970, as amended, 15 U.S.C. §§ 1681-1681(u). Includes provisions to reduce identity theft and to help victims of identity theft to recover. Title I of the Act covers Identity Theft Prevention and Credit History Restoration. Title VII covers Relation to State Laws (preemption).

(http://www.ftc.gov/os/statutes/050131fcra.pdf.)

Summary of FTC actions under the Fair Credit Reporting Act and Fair and Accurate Transactions Act: (http://www.ftc.gov/os/statutes/fcrajump.htm)

In February 2005, the FTC published *Guidelines Requiring the Proper Disposal of Consumer Information*. They took effect on July 1, 2005 and cover disposal of consumer reports and information obtained from them. 69 Fed. Reg. 68,690.
http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.pdf

On July 18, 2006, the FTC and the federal banking agencies released for comment proposed Guidelines for Identity Theft Red Flags and Address Discrepancies. When adopted t hey will require financial institutions and creditors reports to develop and implement identity theft prevention programs. 71 Fed. Reg. 40785-40826 (July 18, 2006).
http://www.fdic.gov/news/news/financial/2005/fil705.html

Financial Industries Modernization Act of 1999 (Gramm-Leach-Bliley) –15 U.S.C. §§ 6801-6810 (disclosure of personal financial information), 15 U.S.C. §§ 6821-6827 (fraudulent access)

- Part of broader legislation which removes barriers to banks engaging in a wider scope of financial services.

- Applies to financial institutions' use and disclosure of nonpublic financial information about consumers.

- Very broadly defines "Financial Services."

- Section 501(b) requires administrative, technical, and physical safeguards to protect covered nonpublic personal information.

- Federal banking agencies have promulgated *Interagency Guidelines Establishing Standards for Information Security* for financial institutions subject to their jurisdiction. 66 Fed. Reg. 8616 (February 1, 2001) and 69 Fed. Reg. 77610 (December 28, 2004). The *Guidelines* are published by each agency in the Code of Federal Regulations – Office of the

Comptroller of the Currency, 12 C.F.R., Part 30, App. B; Board of Governors of the Federal Reserve System, 12 C.F.R., Part 208, App. D-2 and Part 225, App. F; Federal Deposit Insurance Corporation, 12 C.F.R., Part 364, App. B; Office of Thrift Supervision, 12 C.F.R., Part 570, App. B, National Credit Union Administration, 12 C.F.R., Part 748, App.

- The Securities and Exchange Commission promulgated Regulation S-P: *Privacy of Consumer Financial Information*, 17 C.F.R., Part 248, for financial institutions under its jurisdiction.

- The Federal Trade Commission has issued a final rule, *Standards for Safeguarding Customer Information*, 16 C.F.R., Part 314, for financial institutions within its jurisdiction.

- Standards were also issued by the Commodity Futures Trading Commission, 17 C.F.R. §160.3.

- Provides for criminal and administrative penalties for violation.

Health Insurance Portability and Accountability Act (HIPAA)
Various provisions in Title 26 U.S.C. and Title 42 U.S.C.

- Part of broader legislation regulating health insurance.

- Privacy regulations, 45 C.F.R., Part 164.530(c), apply to both electronic and non-electronic protected health information, includes the "mini-security" rule, which requires "appropriate administrative, technical and physical safeguards."

- More detailed *Security Standards for the Protection of Electronic Protected Health Information*, 45 C.F.R., Part 164, Subpart C become effective on April 20, 2005, (April 20, 2006 for small health plans).

- Privacy and security requirements apply to healthcare providers' use and disclosure of nonpublic health information.

– Provides for criminal and administrative penalties for violation.

Children's Online Privacy Protection Act of 1998
15 U.S.C. §§6501-6506

– Regulates online collection and disclosure of information from children under 13 years of age.

– Requires regulations requiring "reasonable procedures to protect the confidentiality, security and integrity" of covered information. 15 U.S.C. §6502.

– The implementing regulations are published at 16 C.F.R., Part 312. Section 312.8 requires "reasonable procedures to protect the confidentiality, security and integrity" of covered information.

– Violations are treated as unfair trade practices under the Federal Trade Commission Act, 15 U.S.C. §57a.

Federal Trade Commission Act
The Federal Trade Commission has used its general power to stop unfair and deceptive trade practices under Section 5 of the Federal Trade Commission Act, 15 U.S.C. §41, in the area of consumer privacy and security. For example, the FTC has brought enforcement actions against companies which did not follow their posted website privacy and security policies, alleging deceptive trade practices. See, www.ftc.gov/privacy/index.html.

A significant recent FTC case is *In re: BJ's Wholesale Club, Inc.* in which the FTC alleged that it was an unfair trade practice for BJ's to fail to take reasonable security measures to protect credit card and debit card purchase information, even in absence of a posted policy. The settlement included a requirement of establishing and maintaining a comprehensive information security program, with outside security audits every two years for 20 years. See,. http://www.ftc.gov/opa/2005/06/bjswholesale.htm.

Government Information Security Reform Act of 2001
44 U.S.C. §101 nt.
Information security requirements for federal agencies, including risk assessment and reporting of information security status, including deficiencies.

Federal Information Security Reform Act of 2002
44 U.S.C. §3544(a)(1)(A).

- Part of the E-Government Act of 2002.

- Requires the Director of the Office of Management and the Budget to require federal agencies to identify and establish information security plans and procedures based on risk.

- Can apply to government contractors through regulations or contracts.

Sarbanes - Oxley
Pub. L. No. 107-204 (2002); various provisions in 15 U.S.C.

- A broad based law, passed in response to high profile incidents of corporate misconduct, which, *inter alia*, establishes enhanced recordkeeping and reporting requirements for publicly traded companies and their auditors.

- Sections 302 and 404 and the SEC Rules implementing them, which are contained in 17 C.F.R., Parts 210, 228, 229, 232, 240, 249, 270 and 274, include requirements for reporting on the company's "internal controls over financial reporting," including assessing the effectiveness of controls, reporting on weaknesses in controls and personal certification by the chief executive officer and chief financial officer. The company's outside auditor must attest to and report on the company's assessment of internal control .

- While the Act does not contain express information security provisions, it is generally accepted that adequate information security relating to financial controls is necessary to comply with these requirements.

B. Pennsylvania Laws

Wiretapping and Electronic Surveillance Control Act
19 Pa. C.S.A. §§5701, et seq.

Hacking and Similar Offenses
18 Pa. C.S.A. §7611, et seq.

- Computer Theft (unlawful access) §7613

- Unlawful Duplication of Computer Data §7614

Breach of Personal Information Notification Act
73 P.S. §§2301-2329

Generally requires notice, without unreasonable delay, to Pennsylvania residents" whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person" through breach of security of a computerized system.

C. Other States' Laws

Breach Notification

A state law which has been credited with public disclosure of many of the recent incidents of consumer information compromise is a recent California law, Cal. Civ. Code §§ 1798.29(a), 1798.82(a), (Senate Bill 1386), that requires businesses that conduct business in California and state agencies to notify individuals whose personal information has been compromised. Earlier data compromises, similar to some of the current ones, were reportedly not disclosed before the California law became effective. Other states are also enacting and considering similar laws. At least thirty-four states have adopted data breach notification laws. Twenty-four states now have credit freeze laws which permit consumers to freeze their credit reports from access for new credit or all access. There are differences among the laws adopted by the various states. The National Conference of State Legislatures maintains a database of state statutes and proposed legislation to address identity theft. (http://www.ncsl.org/programs/lis/privacy/idtheft.htm). The Public Interest Research Group (PIRG) has an online summary of state security freeze and security breach notification laws. (http://www.pirg.org/consumer/credit/statelaws.htm).

Reasonable Security Requirements

Another California law, Cal. Civ. Code § 1798.81.5, (Assembly Bill 1950), imposes a general requirement of "reasonable security procedures and practices" on businesses that own or license certain kinds of personal information about California residents. Several other states, including Arizona, Nevada, Rhode Island, Texas and Utah, have adopted similar laws.

Secure Disposal

California also requires businesses to take reasonable steps to destroy records (paper and electronic) containing certain kinds of personal information which is no longer required to be retained. The records must be shredded, erased or modified to make then undecipherable by any means. Cal. Civ. Code § 1798.1. Arkansas, Kentucky, Hawaii, New Jersey, North Carolina, Texas and Utah have enacted similar legislation.

III. Selected Information Security Cases

United States v. Phillips, 2007 WL 172131 (5th Cir. 2007)
(Student who used university's network to access hundreds of computers and steal information from them violated the Computer Fraud and Abuse Act. Violation of the acceptable use policy made the access "unauthorized.")

Fibre Systems International v. Roehrs, 2006 WL 3378403 (5th Cir. 2006)
(Civil action against former employee who allegedly stole sensitive information from information systems. Civil damage actions are available to enforce all prohibited conduct under the Act; they are not limited to one specific section.)

In the Matter of Guidance Software, Inc., FTC File No. 062 3057 (Settlement, approved November 16, 2006).
(Settlement of claim that a software company engaged in deceptive trade practices where it failed to take reasonable security measures to protect sensitive customer, in contrast to security representations on its website. Hackers accessed credit card information on thousands of customers. The settlement bars future misrepresentations and requires establishing and maintaining a comprehensive information security program, with outside audits. This is the FTC's fourteenth enforcement action involving information security.)

Butera & Andrews v. IBM, Inc., 2006 WL 2971107 (D. D.C. 2006).
(Claim by a law firm under the Computer Fraud and Abuse Act, alleging 42,000 attacks on its e-mail server from IP addresses controlled by IBM. Motion to dismiss granted on the ground that an employer is not liable for an employee's unauthorized violations of the act, without the employer's knowledge. Violations must be "intentional" which requires knowing and conscious activity.)

Forge Industrial Staffing, Inc. v. De La Fuente, 2006 WL 2982139 (N.D. Ill, 2006).
(Civil action by an employer under the Computer Fraud and Abuse Act. Motion to dismiss denied. Use of company computer to set up a competing business and to attempt to alter and destroy data was "unauthorized" access. Breach of fiduciary duty of loyalty negates authorization.)

Wilson v. Moreau, 2006 WL 2171563 (D. R.I. 2006)
(Litigation costs do not count toward the $5,000 minimum damages amount under the Computer Fraud and Abuse Act.)

Inventory Locator Service, LLC v. Partsbase, Inc., 2006 WL 1646091 (W.D. Tenn. 2006).
(Claims and counterclaims under the Computer Fraud and Abuse Act in which the parties each alleged that the other party unlawfully accessed its database. The plaintiff alleged that the defendant fabricated evidence by altering server logs to show intrusions

which never occurred. The court appointed a special master to determine the authenticity of the server logs.)

Nilfisk-Advance, Inc. v. Mitchell, 2006 WL 827073 (W.D. Ark. 2006).
(On motion to dismiss, allegations that an engineer transmitted confidential new product information from his work computer to his home computer, with the intent of conveying it to competitors, state claims under the Computer Fraud and Abuse Act.)

Expert Business Systems, LLC v. BI4CE, Inc., 411 F.Supp. 2d 601 (D. Md. 2006).
(Summary judgment granted for defendant in case under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act involving a dispute between former joint venturers. The court found that there was an utter lack of substantial evidence to support allegations that the defendants intercepted e-mails and planted a Trojan Horse to gain unauthorized access to plaintiffs' computers.)

United States v. Millot, 433 F.3d 1057 (8th Cir. 2006).
(Criminal prosecution under the Computer Fraud and Abuse Act. A computer security contractor, to which security management has been outsourced, can be a "victim" in a computer intrusion and can incur "a loss." The loss does not have to be suffered by the owner of the system.)

Spangler, Jennings & Dougherty, P.C. v. Mysliwy, 2006 ILR Web (P&F) 1513, No. 2:05cv/08 (N.D. Ill. 2006).
(Civil action by law firm under the Computer Fraud and Abuse Act against former partner who took computer files. Summary judgment for law firm denied where it failed to show damage from impairment of the computers data or systems. Only established damages were time and money to assess what data was taken and what the defendant did with it.)

International Airport Centers LLC v. Citrin, 440 F.3d 420 (7th Cir. 2006).
(Civil action by employer against former employee under the Computer Fraud and Abuse Act. Employee exceeded authority when he breached duty of loyalty by using a secure-erase program to delete data from his laptop before he quit to go into business for himself. Use of the erasure program was a "transmission.")

U.S. v. ChoicePoint, Inc., FTC File No. 052-3069 (N.D. Ga. 2006).
(FTC court enforcement action in which the FTC alleged that the defendant committed unfair trade practices under the Federal Trade Commission Act and violated the Fair Credit Reporting Act by selling personal information to subscribers who turned out to be criminals, despite obvious red flags. The subscribers purchased the information to commit identity theft and information concerning more than 163,000 consumers was compromised. A stipulated judgment included a $10 million civil penalty, a $5 million fund for consumer redress, and a requirement for a comprehensive information security program, with independent audits every 2 years for 20 years. It also requires procedures to ensure that consumer reports are provided only to those with a permissible purpose.)

American Bar Ass'n v. Federal Trade Commission, 430 F.3d 457 (D.C. Cir. 2005).
(Gramm-Leach-Bliely privacy requirements do not apply to the practice of law.)

Corbell v. Norton, 2005 WL 2665629 (D.D.C. 2005).
(U.S. Department of the Interior's fiduciary duty to administer Indian trust accounts included the duty to provide adequate information security. Court entered an injunction requiring that all systems containing confidential account information must be disconnected from the Internet, all intranet connections, other department systems and contractor and tribe systems until they are secured. Includes a detailed discussion of information security requirements for federal agencies.)

DIRECTV, Inc. v. Pepe, 2005 WL 3436625 (3rd Cir. 2005).
(Satellite television service provider brought action based on unauthorized interception of its signal through pirate descrambling equipment. Satellite television signals were "electronic communications" under the Electronic Communications Privacy Act. Private right of action for damages is available.)

In the Matter of DSW, Inc., FTC File No. 052-3096.
(Settlement approved December 1, 2005).
(Settlement of a complaint that a retailer engaged in "unfair" trade practices, in violation of the Federal Trade Commission Act, by failing to provide reasonable and appropriate security for sensitive customer information. Settlement requires establishing and maintaining a comprehensive information security program, including third-party audits.)

P.C. Yonkers, Inc., et al. v. Celebrations The Party and Seasonal Superstore, LLC, 2005 WL 2931940 (3rd Cir. 2005).
(Claim under the Computer Fraud and Abuse Act against a former employee who allegedly accessed the plaintiff's computer system to gain information to go into competition. Denial of injunction affirmed where there was evidence of access only and no evidence of what information was viewed or taken. Reviews standards for injunctive relief and compensatory damages.)

Charles Schwab & Co., Inc. v. Carter, 2005 WL 2369815 (N.D. Ill. 2005).
(Action under the Computer Fraud and Abuse Act against a competitor which allegedly hired a key employee of the plaintiff and allegedly directed him to download proprietary information before he left. An action under the CFAA may be based on vicarious liability.)

Secure Info Corp. v. Telos Corp., 2005 WL 2218424 (E.D. Va. 2005).
(Action under the Computer Fraud and Abuse Act against competitors based on an allegation that they hired a consultant to deliver software to them for analysis, in violation of the software's license agreement. No violation of the CFAA where consultant's access was authorized and he later made unlawful use of it.)

Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Matsuda, 2005 WL 2254002 (D.Md. 2005).
(Access by a union officer to confidential information to provide it to a competing union did not violate the Computer Fraud and Abuse Act or the Stored Wire and Electronic Communications Access Act.)

Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd., 2005 WL 218515 (S.D.N.Y. 2005).
(Lost profits and lost commercial advantage are not "losses" under the Computer Fraud and Abuse Act. Covers only damage to or impairment of a computer system.)

In the Matter of BJ's Wholesale Club, Inc., FTC File No. 042-3160; (settlement approved September 23, 2005).
(Settlement of complaint that a retailer engaged in "unfair" trade practices, in violation of the Federal Trade Commission Act, by storing and transmitting credit card and debit card information in an insecure manner. Settlement requires establishing and maintaining a comprehensive information security program, including third party audits. A significant case because it is the first one in which the FTC alleged that failure to provide adequate security for consumer information is an unfair trade practice. Past enforcement actions involved breach of privacy and security promises and violation of privacy and safeguards regulations by covered entities under laws like Gramm-Leach-Bliley.)

U.S. v. Councilman, 418 F.2d 67 (1st Cir. 2005) (en banc).
(Reversing a district court decision and panel affirmance, the First Circuit held, en banc, that interception of an e-mail message in temporary storage incident to transmission states a violation of the Wiretap Act as amended by the Electronic Communications Privacy Act. The case is a criminal prosecution of a vice-president of an Internet booklisting service that provided e-mail to subscribing booksellers, based on alleged interception of incoming e-mails from Amazon.com which were reviewed for commercial advantage.)

Creative Computing v. Getloaded.com, 386 F.3d 930 (9th Circ. 2004).
(Action under the Computer Fraud and Abuse Act in which a competitor of a website for matching trucks with loads, set up a competing website, used its customers logons and passwords to get unauthorized access to competitive information, used an unpatched vulnerability to get backdoor access and examine proprietary sourcecode and had an employee access confidential information before he left. "Damage" does not have to be from a single incident and may include loss of business and good will.)

Theofel v. Farley Jones, 359 F.3d 1066 (9th Cir. 2004).
(Use of a patently overbroad subpoena in a civil action to obtain e-mails from an Internet Service Provider, which were in backup storage, was a violation of the Stored Communications Act.)

Fraser v. Nationwide Mutual Ins., 352 F.2d 107 (3rd Cir. 2004).
(Insurance agent brought claim against insurance company under the Electronic Communications Privacy Act based on a claim that the company accessed his e-mails which were stored on its server. The court held that there was no violation of the Act because there was no interception of the e-mail during transit. There also was no violation of the Stored Communications Act because the company was covered by the exception for service providers.)

United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003).
(Search warrant based on evidence of child pornography seized by a private hacker did not violate a defendant's Fourth Amendment rights where hacker did not act as agent of police; unauthorized access through transmission of a Trojan Horse to a child pornography newsgroup did not violate the Electronic Communications Privacy Act.)

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).
(Employer did not violate the Electronic Communications Privacy Act by accessing and viewing the contents of any employee's secure website because no electronic communication was intercepted during transmission. The unauthorized access did constitute a violation of the Computer Fraud and Abuse Act.)

United States v. Ropp, 2004 WL 2823039 (C.D. Cal. October 7, 2004).
(Defendant installed a hardware keylogger on the computer of an insurance company's employee which was connected to its network. Defense motion to dismiss charges under the Electronic Communications Privacy Act was granted on the ground that data between the keyboard and CPU was not a message in transmission in interstate commerce.)

George S. May Int'l Co. v. Hostetler, 2004 WL 1197395 (N.D. Ill. May 28, 2004).
(Claim that former employee accessed a company's computer system to take copyrighted materials with him when he left to start a competing business states a claim under the Computer Fraud and Abuse Act.)

I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004).
(Claim against a competitor under the Computer Fraud and Abuse Act alleging that defendant accessed the plaintiff's subscription website and copied content; wrongful access and copying constitutes "damage" under the Act.)

Physicians Interactive v. Lathian Systems, Inc., 2003 WL 23018270 (E.D. Va., December 5, 2003).
(Preliminary injunction granted under the Computer Fraud and Abuse Act where plaintiff made a preliminary showing that a competitor hacked its website by sending bots to collect customer lists and proprietary software.)

Pearl Investments, LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326 (D. Me. 2003). (Summary judgment granted against plaintiff in a case under the Computer Fraud and Abuse Act based on a claim that the defendant, which had developed a new automatic trading system for the plaintiff, made unauthorized access into the system to obtain trading information. The plaintiff failed to produce evidence that the defendant damaged its system in any quantifiable amount.)

IV. Selected Data Compromise Cases[2]

Mace v. TJX Cos., Inc., 1:07-cv-10162 (D. Mass.)
(Consumer class action filed on January 29, 2007, alleging negligence for retailers' failure to follow the Payment Card Industry Security Standard. Hackers reportedly obtained access to debit and credit card information.)

AmeriFirst Bank v. TJX Cos., Inc., No. 1:07-cv-10169 (D. Mass.)
(Class action by banks against retailers to recover costs of responding to breach which was allegedly caused by negligent information security practices. Claims include contract, negligence and negligence per se. The negligence per se claim is based on failure to comply with the Gramm-Leach-Bliley Safeguards Rule. Hackers reportedly obtained access to debit and credit card information.)

Harrington v. ChoicePoint, Inc., No. 05-cv-1294 (C.D. Cal., October 11, 2006)
(Class action under the Fair Credit Reporting Act based on identity thieves obtaining access to personal information by posing as customers. The court dismissed the action because there was no evidence that the plaintiffs' information was communicated. The federal court declined to rule on state consumer protection laws.)

Bell v. Acxiom Corp., No. 4:06CV00458 – WRW (E.D. Ark., October 3, 2006)
(Actual harm is required to support a claim based on theft of personal information by hackers in a data breach. Risk of identity theft and the possibility of receiving junk mail is not a sufficient injury to provide standing to sue.)

Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Oh. 2006)
(Contract and tort class action claims based on data breach. Increased risk of financial harm, by an unknown third party, at an unidentified point in the indefinite future, is too speculative to constitute a cognizable injury to confer standing. In addition, there are no cognizable damages sufficient to state claims in contract, negligence, conversion or breach of fiduciary duty.)

Pennsylvania State Employees Credit Union v. Fifth Third Bank, 2006 WL 1724574 (M.D. Pa. 2006)
(Action by credit card issuer against retailer's credit card processor to recover costs of replacing cards that had been compromised in the retailer's computer system. Court granted summary judgment on the final remaining claim against the retailer's credit card processor – a contract claim. The court held that the issuer is not a third-party beneficiary of the contract between the processor and Visa. The opinion

[2] Originally prepared with Samuel J. Stoller, a law student at Ohio State University, Moritz College of Law and a 2005 summer associate (now an associate) at Thorp Reed & Armstrong, LLP.

discusses Visa's dispute resolution procedures under which some of the losses were charged to the processor.)

Sovreign Bank v. B.J.'s Wholesale Club, Inc., 2006 WL 1722398 (M.D. Pa. 2006)
(Issues and rulings the same as *Pennsylvania State Employees Credit Union* opinion above.)

Jones v. Commerce Bankcorp, Inc., 2006 WL 1409492 (S.D.N.Y. 2006)
(Action by bank customer to recover for losses allegedly caused by theft of confidential data by bank employees. In ruling on a motion to dismiss, the court held that the plaintiff stated claims for negligence, breach of fiduciary duty and breach of contract. The court dismissed claims for infliction of emotional distress, commercial bad faith and consumer fraud.)

Guin v. Brazos Higher Education Service Corp., No. 05-668 (D. Minn., February 2, 2006)
(Action against loan service provider based on theft of laptop with unencrypted personal financial data from employee's name. No duty to encrypt data under Gramm-Leach-Bliley where there was a security policy in place. Heightened risk of identity theft is insufficient to support a negligence action.

Pennsylvania State Employees Credit Union v. Fifth Third Bank and BJ's Wholesale Club, Inc., 2005 WL 3040778 (M.D. Pa. 2005).
(Action by credit card issuer against retailer and retailer's credit card processor to recover costs of replacing cards that had been compromised in the retailer's computer system. Credit card issuer does not have claims against retailer in contract, negligence, equitable indemnification or unjust enrichment. Card issuer has a contract claim against the retailer's card processor, as a third-party beneficiary to the card processor's contract with Visa.)

(In an earlier decision, 2005 WL 1154594, the court addressed the retailer's third-party claim against its software provider. The retailer alleged that the software improperly retained credit and debit card information after transactions were processed. Ruling on a motion to dismiss, the court permitted claims to proceed based on breach of contract, breach of warranty and negligence. These claims were limited to the value of the compromised cards as blanks. Claims based on indemnity or contribution, declaratory judgment and state consumer protection laws were dismissed. All claims were subsequently dismissed when the retailer was dismissed from the action.)

Sovereign Bank v. BJ's Wholesale Club, Inc. and Fifth Third Bank, 395 F. Supp. 2d 183 (M.D. Pa. 2005).
(Action by credit card issuer against retailer and retailer's credit card processor to recover costs of replacing cards that had been compromised in the retailer's computer system. Only a negligence claim may be brought against the retailer.

Claims based on third-party beneficiary to contract, equitable indemnification and unjust enrichment were dismissed. Claim against card processor based on contract, as third-party beneficiary to contract between card processor and Visa, may proceed. Claims for negligence and equitable indemnification were dismissed).

Banknorth, N.A. v. BJ's Wholesale Club, Inc., 2005 WL 1610654 (D. Me. July 8, 2005).
(A credit card issuer may bring claims based on contract, tort and equitable subrogation against a retailer based on allegations of improper storage of credit card information in its computers which allowed hackers to obtain the information.)

CardSystems Solutions, Inc. Litigation (Cal. Sup. Ct., filed June 27, 2005).
(Class action against CardSystems, credit card associations and a card-issuing bank on behalf of credit card holders and merchants which accepted cards. The claims include negligence in security of credit card processing systems and failure to inform consumers about the security breach in a timely manner.)

Harrington v. ChoicePoint, Inc., No. CV05-1294 (SJO) (JWJX) (C.D. Cal., filed Feb. 22, 2005)
(A federal class action lawsuit based on allegations that ChoicePoint failed to maintain adequate security procedures to avoid disclosing credit and financial information about 145,000 individuals to unauthorized third parties, resulting in identity theft. It includes claims under the federal Fair Credit Reporting Act, the California Credit Reporting Agencies Act and the California Unfair Competition Law. (One of 3 actions pending in the same court.))

AHLO Inc. v. Bank of America Corp., No. 05-2538-CA27 (Fla. Cir. Ct., filed Feb. 3, 2005).
(Action by a small business to recover against its bank for losses from the unauthorized electronic transfer from its account to a bank in Latvia. The claims include breach of good faith and fair dealing (in contract), breach of fiduciary duty (in selling an insecure online account), negligence (in security, training, verification and response to the incident) and fraud.)

Bell v. Michigan Council 25, AFSCME, No. 246684, 2005 LEXIS 353 (Mich. Ct. App. Feb. 15, 2005) (unpublished).
(The plaintiffs, who were all members of the defendant union, became victims of identity theft when the daughter of the union treasurer obtained lists of the plaintiffs' personal information and participated in the appropriation of their identities. The court affirmed the jury's decision in favor of the plaintiffs and held that, under the circumstances of the case, the defendant did owe the plaintiffs a duty to ensure the security of the confidential underlying information.)

Lukens v. Dunphy Nissan, Inc., Civil Action No. 03-767, 2004 U.S. Dist. LEXIS 14528 (E.D. Pa. July 23, 2004).

(The plaintiff consumer filed an action alleging that the defendant auto dealer had violated the Fair Credit Reporting Act when it hired a known identity thief who used the plaintiff's credit information to open fraudulent accounts in the consumer's name. The defendant filed a motion for partial summary judgment relating to the FCRA claims. The court denied the motion, holding that dealer could be held vicariously liable for the acts of the employee because the agency relation contributed to the identity theft and the dealer provided access to personal credit information to a known identity thief.)

Schuchart & Rheinstein v. La Taberna del Alabardero, Inc., No. 03-7105, 2004 U.S. App. LEXIS 7545 (D.C. Apr. 20, 2004).
(One of the plaintiff customers used her personal credit card to pay for lunch at the defendant's restaurant. The defendant provided a copy of the credit card receipt to the customer's employer without the consent of the customer and the plaintiff sued the defendant alleging the tort of intrusion upon seclusion. Due to the public importance of matter, the D.C. Court of Appeals exercised its discretion to certify questions of law. The questions certified included whether a customer stated a claim for intrusion upon seclusion when a business disclosed a customer's personal credit card information to a third party not involved in processing payment without the customer's consent.)

Kuhn v. Capital One Fin. Corp., 18 Mass. L. Rep. 524 (Mass. Super. Ct. 2004).
(Computer hacker broke into Capital One's website server, appropriated the plaintiff's identity, and opened approximately 18 fraudulent accounts in the customer's name. The court granted Capital One's motion for summary judgment on all counts, holding that the privacy notice in the customer's agreement did not provide a guarantee against identity theft and that nothing in the record implied that Capital One caused the identity theft. In addition, the court stated that under Massachusetts law, the relationship of a bank to its customers has traditionally been viewed as that of creditor and debtor, a relationship which imposes no corresponding duty on Capital One to make disclosures to their customers in this instance.)

Garay v. United States Bancorp**,** 303 F. Supp. 2d 299 (E.D. N.Y. 2004).
(The plaintiff consumer sued the defendant bank for aiding and abetting an identity theft pursuant to the Identity Theft and Assumption Deterrence Act of 1998, stemming from the bank's issuance of a credit card in the plaintiff's name to an imposter. The court granted the bank's motion for summary judgment, stating that the statute was criminal in nature and provided no private right of action.)

Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).
(The court of appeals affirmed the district court's granting of a motion of summary judgment in favor of the defendant. The plaintiff was the victim of identity theft when a third party created a matchmaking profile in the name of the plaintiff on the defendant's internet dating service website. The plaintiff began receiving threatening and sexually explicit communications in response to the imposter

profile. The court of appeals held that the Internet dating service was statutorily immune from the victim's suit, as the defendant was not an Internet Content Provider and did not play a significant role in the creation or development of the relevant information.)

Higgins v. Citibank, N.A., 585 S.E. 2d 275 (S.C. 2003).
(The plaintiff, an identity theft victim, sued 3 banks claiming that they negligently issued credit cards, in the plaintiff's name, to an imposter. The court held that a bank owes no duty to non-customers whose personal information is used through identity theft to obtain credit cards from the bank. The relationship is far too attenuated to create a legal duty.)

Stollenwerk v. TriWest Health Alliance Corp., No. 2:03cv00185 (D. Ariz. Oct. 20, 2003)
(During a burglary of a government contractor which runs a Defense Department health maintenance organization, thieves stole computer hard drives which contained personal information concerning about 562,000 military personnel, including medical claim histories and Social Security numbers. The court dismissed a class action complaint, finding that "[w]ithout damages, it doesn't matter how negligent anyone was . . . ." The court provided the opportunity for plaintiffs to file an amended complaint.)

Bodah v. Lakeville Motor Express, Inc., 663 N.W. 2d 550 (Minn. 2003).
(The safety director of a trucking company sent a facsimile containing the names and social security numbers of 204 employees to managers of 16 freight terminals. The employees filed a class action lawsuit against the employer alleging the tort of invasion of privacy. The Supreme Court of Minnesota held that the court of appeals erred in reversing the dismissal of the complaint because the dissemination of the information did not constitute the requisite "publicity" under Minnesota law to support the claim. In dicta, the court noted that if the transmission of the data actually resulted in a pecuniary loss due to identity theft, the plaintiff would have been able to bring a negligence action against the employer.)

Rice v. Wal-Mart Stores, Inc., Civil No. 02-390-B, 2003 U.S. Dist. LEXIS 17288 (N.H. Sept. 30, 2003).
(The plaintiff widows sued the defendant employer for using its employee's names and confidential medical information without their consent in order to implement a corporate-owned life insurance (COLI) plan. The court cited *Remsburg v. Docusearch, Inc.* in denying the widows' claim for commercial appropriation, because Wal-Mart did not exploit the employee's reputations or prestige when it purchased COLI policies in their names. However, the court denied Wal-Mart's motion to dismiss the breach of fiduciary duty claim, noting the plaintiff's allegation that Wal-Mart profited when it misused the confidential and personal information of the employees and that the employees were injured as a result.)

***Smith v. Citibank**,* No. 00-0587-CV-W-1-ECF, 2001 U.S. Dist. LEXIS 25047 (W.D. Mo. October 3, 2001).
(In this case, a non-customer plaintiff alleged that the defendant bank was negligent in opening a credit account in the plaintiff's name and in investigating disputes regarding amounts due on the account. The court granted the defendant's motion for summary judgment regarding the plaintiff's negligence claims, holding that the bank owed no duty to the plaintiff because he was a non-customer. In addition, the court noted that the defendants had no duty to investigate the plaintiff's disputes because the duty to investigate arose only after a consumer reporting agency provided the bank with a notice of dispute.)

***Polzer v. TRW, Inc.**,* 682 N.Y.S. 194 (N.Y. App. Div. 1998).
(The plaintiffs sought review of an order granting summary judgment to defendant bank and credit corporation. The causes of action proposed by the plaintiffs included the negligent enablement of imposter fraud, when an imposter stole the plaintiffs' credit information, and fraudulently obtained credit cards. The court affirmed the judgment, holding that New York did not recognize a cause of action for the negligent enablement of imposter fraud. In addition, the court held that the plaintiffs failed to state a claim in negligence, because the bank had no special relationship with the plaintiffs, as they stood only in a creditor/debtor relationship.)

For further discussion of these issues, see:

- Brendan Delany, "Comment: Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Imposter Fraud," *54 Cath. U.L. Rev. 553* (Winter, 2005)

- Holly K. Towle, "Identity Theft: Myths, Methods and New Law," *30 Rutgers Computer & Tech. L. J. 237* (2004)

V. Information Security Legal Resources

A. Online Resources

BNA Electronic Commerce & Law Report (online legal report, also available in print), www.bna.com

BNA Privacy & Security Law Report (online legal report, also available in print), www.bna.com

Federal Trade Commission, www.ftc.gov, see particularly www.ftc.gov/privacy/privacyinitiatives/safeguards.html

Glasser Legal Works, *The Cyberspace Lawyer*, (law report covering Internet topics, also available in print), www.legalwks.com

Glasser Legal Works, *Privacy and Information Law Report*, (law report covering privacy laws and technologies), www.legalwks.com

Pike & Fischer, *Internet Law & Regulation* (online subscription website containing indices, articles and cases), http://Internetlaw.pf.com

SANS Institute (an international organization devoted to security research, education and certification), www.sans.org

U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), www.cybercrime.gov

B. Print Materials

American Institute of Certified Public Accountants, *Information Security Management and Assurance: A Call to Action for Corporate Governance*, available at www.aicpa.org

Kevin Cronin and Ronald N. Weikers, *Data Security and Privacy Law: Combating Cyberthreats* (West Spring 2006 Supp.) (looseleaf treatise, periodically updated) (**recommended for a comprehensive treatment of the legal and practical issues**)

Cyber Security Industry Alliance, *Sarbanes-Oxley Act: Implementation of Information Technology and Security Objectives* (December 2004) available at www.csialliance.org

D. Reed Freeman, Jr., "Information Security for In-House Counsel," *6 Briefly 1-35* (December 2002) (National Legal Center For Public Interest)

Lawrence Gordon, et al., *2006 CSI/FBI Computer Crime and Security Survey* (Computer Security Institute 2006) (available at www.gocsi.com)

Robert V. Hale II, “Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet,” *21 Santa Clara Computer & High Tech. L. J. 543-559* (March 2005)

International Organization for Standardization (ISO), www.iso.org, has published several standards for comprehensive security programs, information security and evaluation; see particularly ISO/IEC 17799:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management and ISO/IEC 27001 – Information Technology – Security Techniques – Information Security Management Systems - Requirements

Internet Security Alliance, *Contracting for Information Security in Commercial Transactions* (2005)

IT Governance Institute, *Control Objectives for Information and Related Technology (COBIT 4.0)* (2005), a framework for internal control systems which includes information security, available at www.isaca.org/cobit.htm

Erin Kenneally, “It Depends: Defining Legal Values for Network Behavior,” *login: The Magazine of USENIX & SAGE* (December 2002)

Erin Kenneally, “Stepping on the Digital Scale – Duty and Liability for Negligent Internet Security,” *login: The Magazine of USENIX & SAGE* (December 2001)

Erin Kenneally, “Who’s Liable for Insecure Networks?” *Computer* (June 2002) (Institute of Electrical and Electronics Engineers)

Kimberly Kiefer, et al., *Information Security: A Legal, Business and Technical Handbook* (American Bar Ass’n 2004) (**recommended for a concise overview of legal and practical issues**)

Kimberly Kiefer and Randy Sabett, “Openness of Internet Creates Potential for Corporate Information Security Liability,” *BNA Electronic Commerce and Law Report* (June 12, 2002)

Mark G. Milone, *Information Security Law: Control of Digital Media* (Law Journal Press 2006) (looseleaf treatise, to be periodically updated) (**recommended for a comprehensive treatment of the legal and practical issues**)

Bruce H. Nearon, et al., “Life After Sarbanes – Oxley: The Merger of Information Security and Accountability,” *4 Jurimetrics 329 – 412* (Summer 2005) (American Bar Ass’n)

Sharon Nelson, David Isom and John Simek, ed., *Information Security for Lawyers and Law Firms* (American Bar Ass’n 2006)

Organization for Economic Co-Operation and Development, *Guidelines for the Security of Information and Networks: Towards a Culture of Security* (2002)

Stewart Personick and Cynthia Patterson, eds., *Critical Information Infrastructure and the Law* (National Academics Press 2003)

E. Michael Power and Rowland L. Trope, *Sailing in Dangerous Waters: A Director's Guide to Data Governance* (American Bar Ass'n 2005)

Charles Raul, et al., "Liability for Computer Glitches and Online Security Lapses," *BNA Electronic Commerce & Law Report* (August 2001)

Bruce Schneier, "Liability Changes Everything" (Heise Security, November 2003)

Bruce Schneier, "Hacking the Business Climate for Network Security," *Computer* (April 2004) (Institute of Electrical and Electronics Engineers)

Thomas J. Smedinghoff, "The Coming Expansion of Corporate Information Security Obligations," *BNA World Data Protection Report* (April 2005)

Thomas J. Smedinghoff, "The New Law of Information Security," *The Computer and Internet Lawyer* (November 2005)

Bruce P. Smith, "Hacking, Poaching and Counterattacking: Digital Countermeasures and the Contours of Self-Help," *1 Journal of Law, Economics & Policy 171-195* (Winter 2005)

June Sullivan, *HIPAA: A Practical Guide to the Privacy and Security of Health Data*, (American Bar Ass'n 2004)

Nancy Tribensee, "Liability for Negligent Security – Implications for Policy & Practice," Chapter 4 in Mark Luker and Rodney Peterson, eds., *Computer and Network Security in Higher Education* (John Wiley & Sons, Inc. 2003)

Rowland L. Trope, "Directors' Digital Fiduciary Duties," *Security & Privacy* (January/February 2005) (Institute of Electrical and Electronics Engineers).

U.S. Secret Service, CSO and CERT®, *2006 E-Crime Watch Survey,* available at www.cert.org

Thomas P. Vartanian, et al., "Not On My Watch – When Are Companies Liable for Security Breaches of Their Information Systems," *Electronic Banking Law and Commerce Report* (June 2005)

Jody R. Westby, ed., *Roadmap to an Enterprise Security Program* (American Bar Ass'n 2005)

Benjamin Wright, *Business Law and Computer Security* (SANS Press 2003)

Scott C. Zimmerman, Ron Plesco and Tim Rosenberg, "Downstream Liability for Attack Relay and Amplification," presentation, RSA Security Conference (2002), available at http://www.cert.org/archive/pdf/Downstream_Liability.pdf

C. Course Materials

American Bar Ass'n, "Cyber Security Liability: A Growing Legislative Trend," ABA Annual Meeting, August 8, 2004

American Bar Ass'n, "Information Security and Dealing with Security Breaches," webcast, October 25, 2005

American Bar Ass'n, "Information Security and the Law," webcast, July 20, 2004

American Bar Ass'n, "In the Wake of ChoicePoint: A Discussion of Data Regulation and Security," webcast, April 28, 2005

American Bar Ass'n, "Sarbanes-Oxley – What You Don't Know About Information Security Can Hurt You," ABA Annual Meeting, August 8, 2004

American Bar Ass'n, "Self-Help on the Internet: The Law, Ethics and Tactics of Hacking Back Against Computer Attack," ABA Annual Meeting, August 7, 2004

Boston Bar Association, "Data Security and Privacy Law," course materials, April, 2003

Georgetown University Law Center/Information Systems Security Ass'n, *Emerging Trends in Information Security and the Law: "Plausible Deniability is Dead,"* November 9-10, 2006

Thomas M. Laudise and Leonard T. Nuara, "Liability for Computer Security and Privacy Breaches. Are They Threats or Just Class Action Pipedreams?" Chapter F in *Technology Law Forum* (Pennsylvania Bar Institute 2005)

Practising Law Institute, "Corporate Counsel Alert Series: Recent Developments in Information Security," webcast, November 30, 2005

Practising Law Institute, *6th Annual Institute on Privacy Law – The Convergence of Privacy & Security* (May-June 2005)

Francis X. Taney, "A Primer on Information Security Law for Lawyers (and Their Clients)," Chapter V in *Technology Law Forum* (Pennsylvania Bar Institute 2006)

Anthony Teelucksingh, “Responding to Cybercrime,” Chapter U in *Technology Law Forum* (Pennsylvania Bar Institute 2006)

SANS Institute, “Legal Liability For Information Security: Ask the Experts,” webcast, April 23, 2003

SANS Institute, “Legal Liability for Security Breaches - and Minimum Standards of Due Care,” webcast, February 26, 2003

D. Reporting Cybercrime

CIO Magazine, “CIO Cyberthreat Response & Reporting Guidelines” (February 2002) (developed jointly with the FBI and U.S. Secret Service), available at www.cio.com/research/security/incident_response.pdf

Federal Bureau of Investigation, www.fbi.gov

U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), www.cybercrime.gov

U.S. Secret Service, www.secretservice.gov

State and Local Police – cybercrime units