Commercial and Corporate
Cite as: Joel B. Hanson, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 Shidler J. L. Com. & Tech. 11 (5/23/2008), *at* <http://www.lctjournal.washington.edu/Vol4/a11Hanson.html>

LIABILITY FOR CONSUMER INFORMATION SECURITY BREACHES: DECONSTRUCTING FTC COMPLAINTS AND SETTLEMENTS

Joel B. Hanson[1]

Abstract

For several years, hackers taking advantage of security holes in the information system of TJX Companies, Inc. stole sensitive credit and debit card information belonging to at least 45.7 million customers. The TJX breach is one of the largest thefts of consumer information in history and is illustrative of the recent wave of security breaches. Private lawsuits against companies that fail to protect consumer information have typically failed. However, the Federal Trade Commission has taken enforcement action against such companies that fail to implement reasonable security measures to protect customers' personal information. These complaints have resulted in settlement agreements requiring the businesses to implement comprehensive security programs, complete with third party auditing, for up to 20 years. This Article analyzes the various types of legal violations alleged by the FTC in security breach cases, the factors cited as contributing to the violations, and the remedies typically agreed upon when the complaints are settled. This Article also distinguishes different violations that may result depending on the type of information stolen through a security breach.

Table of Contents

INTRODUCTION

<1>According to U.S. estimates, an information security breach occurs every three days.[2] Hacker intrusions are the leading cause of security breaches.[3] Insider theft and computer thefts are other major causes.[4] Recent examples of breaches include the security failures at LexisNexis and TJX. The LexisNexis breach resulted in the theft of information belonging to over 300 thousand customers.[5] The TJX security breach resulted in the theft of at least 45.7 million customers' credit and debit card information.[6] This is the largest U.S. data breach to date[7] and could eventually cost TJX $168 million.[8] The FTC recently settled actions against both TJX and the parent company of LexisNexis for their failure to use reasonable measures to prevent the security breaches.[9]

<2>The FTC files complaints against businesses that it believes are to some extent responsible for not implementing reasonable measures to protect customers from security breaches. It has used its "Section 5" authority[10] to file complaints against businesses that have experienced security breaches.[11] The violations alleged by the FTC, and the resulting penalties, may be distinguished according to the type of business and information compromised. FTC complaints arising from consumer information security breaches have typically involved the thefts of debit card and credit card information. Criminals can use this "account level" information to make fraudulent charges against a victim's credit card or bank account that is linked to their debit card.[12] When this kind of information is stolen the FTC complaints allege that the businesses have engaged in unfair or deceptive trade practices.

<3>The FTC has alleged Fair Credit Reporting Act[13] (FCRA) violations when a consumer reporting agency allows social security numbers, dates of birth, and credit histories to be obtained by unauthorized buyers. A breach involving this "identity level" information carries a higher risk to the consumer because the information can be used to commit more advanced identity theft and the fraud can be prolonged.[14] Such FCRA violations are also considered unfair or deceptive trade practices.

<4>The FTC has determined that its Section 5 authority applies to businesses' privacy practices, such as how businesses protect consumer information in their possession. The FTC has filed complaints for Section 5 violations related to consumer information where the business: (1) intentionally violated its privacy policy; (2) failed to employ reasonable security measures as implied or promised by its privacy policy; or (3) had no privacy policy but failed to employ reasonable security measures. To date, the FTC has only targeted companies that have had some kind of actual security failure or have intentionally violated their privacy policies. All of the FTC complaints have involved actual or suspected releases of sensitive consumer information.

PRIVATE LAWSUITS AGAINST BUSINESSES FOR FAILING TO PROVIDE ADEQUATE SECURITY HAVE BEEN LARGELY UNSUCCESSFUL

<5>Private lawsuits attempting to hold businesses liable for the injuries to consumers resulting from security breaches have been generally unsuccessful. While several commentators have argued for common law theories of liability for security breaches,[15] courts have been reluctant to impose such liability.[16]

<6>For example, BJ's Wholesale Club, Inc. (BJ's) and Cardsystems Solutions, Inc. (Cardsystems) had security breaches that led to both FTC complaints and private actions against the businesses. While the FTC complaints led to settlement agreements with significant penalties or concessions by the businesses, four private actions related to those breaches have been dismissed.[17]

<7>It should be noted that while businesses that fail to implement appropriate security precautions have generally not been held liable in private lawsuits, the law is developing and there have been some successes in private lawsuits.[18] Lawsuits against TJX have ended in large multi-million dollar settlements.[19] At least 19 private lawsuits were filed against TJX as a result of the security breach.[20]

THE FTC FILES COMPLAINTS FOR UNFAIR OR DECEPTIVE TRADE PRACTICES AGAINST BUSINESSES AFTER A SECURITY BREACH

<8>Section 5 of the Federal Trade Commission Act[21] grants the FTC the power to take enforcement actions against persons, partnerships, or corporations, but not certain financial institutions, for engaging in unfair or deceptive trade practices.[22] Such practices include those that "cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition."[23]

<9>In 1999, the FTC began to apply Section 5 against companies that intentionally violated their own privacy policies with respect to how they treated consumer data within their possession.[24] In 2002, the FTC began to investigate businesses that failed to implement appropriate security measures, which the FTC alleged also violated their own privacy policies because of statements those businesses made with respect to safety of consumer information.[25] Such complaints were sometimes filed even where there was no actual theft of consumer information. Until 2005, the FTC had only filed these kinds of complaints against companies that had a privacy policy in effect.[26] However, starting with BJ's Wholesale Club in 2005, the FTC has filed complaints against businesses that have failed to employ reasonable and appropriate security measures regardless of whether there was any privacy statement made by the business. In doing so, the FTC is setting a normative baseline for security that all companies subject to the agency's jurisdiction must consider when building their payment and customer information systems.

<10>BJ's, a retail chain, did not have a privacy policy in place for its customers.[27] Nevertheless, after banks noticed thieves were making charges against BJ's customers' accounts, the FTC filed a complaint against BJ's

alleging that BJ's lax security allowed thieves to steal the customers' information.[28] In this latter type of complaint where there is no privacy statement, the FTC has only filed complaints where there is an actual security breach and theft of consumer information. Such complaints allege unfair acts or practices, and do not mention deceptive acts.[29] This is because the FTC often distinguishes between unfair acts and deceptive acts.[30]

<11>After the BJ's Wholesale Club complaint and settlement, and the ensuing complaints and settlements against businesses such as DSW and Cardsystems,[31] it appears the FTC may hold a business liable for failing to employ appropriate security measures regardless of whether there was ever any privacy policy in place for customers. The FTC has done this three times.[32]

<12>To date, each company that has been subject to an FTC complaint for unfair or deceptive trade practices related to consumer privacy has been settled rather than fully litigated. Thus, no court has yet affirmed the FTC's application of Section 5 to the instances discussed in this Article. Some commentators have questioned whether courts would agree with the FTC's application.[33] The broad reach of Section 5 is tempered by a statutory restriction. [34]

<13>However, courts have upheld the FTC's application of Section 5 to a wide variety of business practices. Courts have held that the FTC has broad authority to determine what are unfair or deceptive trade practices.[35] Thirty three states have statutes with language similar to Section 5.[36]

FAILURE TO IMPLEMENT REASONABLE SECURITY MEASURES MAY VIOLATE A BUSINESS'S PRIVACY STATEMENT AND THEREFORE BE A DECEPTIVE TRADE PRACTICE

<14>If a business's privacy policy states that consumer information is private and protected, it may be a violation of Section 5 if that business fails to implement reasonable security measures to protect that information. FTC complaints assert that it is a violation of Section 5 if a business: (a) intentionally violates a promise it makes to consumers in its privacy statement or policy;[37] or (b) represents that it implements reasonable measures to protect personal information but fails to implement such measures.[38] Only the latter type of violation is relevant to security breaches. Generally, the FTC has only alleged the latter type of violation when a business' information security has actually been breached and the breach led to the acquisition of personal information by unauthorized individuals. The two exceptions have been when privacy promises were highly inconsistent with the company's actual practices[39] or when a breach was inevitable and had likely already occurred.[40]

<15>The Petco complaint and settlement with the FTC is a typical example of where a business is alleged to have violated its privacy policy by failing to implement reasonable security measures.[41] Petco, a pet supply retail chain, allowed customers to make credit card purchases through its website.[42] The website promised that the customers' information was "safe" and "strictly shielded from unauthorized access."[43] The FTC alleged that a hacker

successfully accessed customer records, including credit card information, using a commonly known web attack called an SQL attack.[44] The FTC noted that the credit card information was not maintained in an encrypted format.[45] The FTC complaint alleged Petco "failed to implement procedures that were reasonable and appropriate to: (1) detect reasonably foreseeable application vulnerabilities, and (2) prevent visitors from exploiting such vulnerabilities and obtaining unauthorized access to sensitive consumer information."[46] The FTC alleged that such a failure to implement reasonable measures to protect consumer information violated Petco's privacy policy. Therefore, Petco's privacy statement was deemed false or misleading and as such an unfair or deceptive trade practice.[47] Petco, like other businesses that have faced FTC complaints after security breaches, settled with the FTC.[48]

A BUSINESS'S PRIVACY POLICY NEED NOT BE VIOLATED FOR INFORMATION SECURITY PRACTICES TO BE DETERMINED UNFAIR TRADE PRACTICES

<16>FTC complaints relating to security breaches have alleged that businesses "did not employ reasonable and appropriate measures to secure personal information collected at its stores."[49] In all cases, the FTC has alleged this failure is an unfair, rather than deceptive, trade practice under 15 U.S.C. § 45.[50]

<17>Three recent complaints alleging this failure, including those against BJ's and Cardsystems, have not alleged the existence of a privacy statement or policy that was violated.[51] Thus, the FTC may file a complaint against a business that has experienced a security breach regardless of whether the business made any promise to keep consumer information private.

<18>To date, the FTC has only alleged violations of Section 5 due to the failure to employ reasonable security in the absence of any privacy policy when the business' information security was actually breached and unauthorized individuals acquired consumer information.[52]

COMPLAINTS AGAINST BUSINESSES FOR FAILING TO EMPLOY REASONABLE AND APPROPRIATE SECURITY MEASURES, LEADING TO CREDIT AND DEBIT CARD FRAUD

BJ's Wholesale Club, Inc. Complaint

<19>BJ's, a retail chain, recorded and stored customers' names, credit and debit card numbers, and card expiration dates.[53] Banks noticed that thieves were making charges against BJ's customers' credit and debit accounts and were forced to cancel those cards.[54] The FTC alleged that BJ's lax security, such as failing to sufficiently restrict access to its network and improperly storing credit and debit card information, allowed thieves to steal the customers' information.[55] The FTC complaint alleged BJ's "did not employ reasonable and appropriate measures to secure personal information collected at its stores."[56] As in other FTC complaints, the BJ's complaint alleges factors or practices which taken together are a failure to employ reasonable and appropriate security for personal information. In its complaint, the FTC alleged that the company had:

- Created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, in violation of bank rules;
- Not used readily available security measures to limit access to its computer networks through wireless access points on the networks;
- Failed to employ sufficient measures to detect unauthorized access or conduct security investigation;
- Failed to encrypt personal information; and
- Stored customer information in files that could be accessed anonymously by using a commonly known default user ID and password.[57]

<20>The FTC complaint alleged this lack of security apparently resulted in a security breach.[58] The complaint noted that BJ's security failure "caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice."[59]

Cardsystems Solutions, Inc. Complaint

<21>The Cardsystems Solutions, Inc. (Cardsystems) settlement, like BJ's, involved credit and debit card information that could be used for fraudulent purposes.[60] Cardsystems provided merchants with an authorization system to collect and verify credit and debit card transactions. Cardsystems collected customer names, card numbers, expiration dates, and security codes.[61] In 2004 a hacker used what is called an SQL injection attack to install programs on Cardsystems' computer network.[62] Those programs collected credit card and debit card information for tens of millions of customers.[63] In 2005 banks found that thieves had used that information to make millions of dollars of fraudulent charges.[64]

<22>As in BJ's and other complaints, the FTC alleged Cardsystems failed to provide reasonable and appropriate security for personal information stored on its computer network. The FTC reached this conclusion based on a list of factors which "taken together, failed to provide reasonable and appropriate security."[65] The FTC alleged three factors that were identical to three factors alleged in the BJ's complaint.[66] Additionally, Cardsystems was alleged to have failed to:

- Adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks;
- Implement simple, low-cost, and readily available defenses to such attacks; and
- Use strong passwords.[67]

<23>The complaint alleged these failures allowed the hacker to obtain the debit and credit card information used to make fraudulent charges.[68] As in

the BJ's complaint, the FTC stated Cardsystems' security failure was an unfair practice.

THE FTC ALLEGES FCRA VIOLATIONS FOR SECURITY BREACHES INVOLVING CONSUMER INFORMATION AT CONSUMER REPORTING AGENCIES

ChoicePoint Complaint

<24>The ChoicePoint Inc. complaint is unique from the other complaints discussed in this article. ChoicePoint Inc. was subjected to a relatively harsh FTC complaint and settlement because of the nature of ChoicePoint's business and the information that was stolen. ChoicePoint and its subsidiaries sell consumer reports, also known as credit histories.[69] ChoicePoint and its subsidiaries are therefore "consumer reporting agencies" and covered by the FCRA.[70] The breach involved especially sensitive consumer information that was allegedly used for identity theft.[71] The information included more than just credit and debit card information that may be used to commit fraud. Unauthorized individuals obtained personal information of consumers, including names, Social Security numbers, dates of birth, bank and credit card account numbers, and credit histories. The complaint cited evidence that the information was used to commit at least 800 cases of identity theft.[72]

<25>The FTC complaint alleged FCRA violations and unfair acts or practices under Section 5. The complaint used language very similar to the complaints against BJ's and Cardsystems. It alleged ChoicePoint failed to employ reasonable and appropriate measures to secure personal information it sells. ChoicePoint was not victimized by a hacker. Rather, ChoicePoint sold consumer information to unauthorized buyers who misrepresented themselves.[73] ChoicePoint allegedly did not have reasonable policies and procedures to verify the identities and qualifications of buyers of personal information and to detect unauthorized buyer activity.[74]

<26>The FTC complaint further alleged that ChoicePoint had failed to utilize readily available business verification products; failed to examine applications; failed to conduct site visits; and failed to utilize other reasonable methods to detect discrepancies in applications.[75] The complaint also offered a long list of common-sense failures, such as approving information buyers who did not even provide their last name.[76] The complaint also noted that ChoicePoint continued to sell these buyers information after both law enforcement authorities and ChoicePoint employees had identified them as suspicious.[77]

<27>The complaint alleged ChoicePoint violated the FCRA by failing to maintain reasonable procedures to prevent the furnishing of consumer reports for purposes not permitted by the FCRA.[78] It also alleged ChoicePoint violated the FCRA by furnishing a consumer report to persons when it had reasonable grounds for believing that the consumer reports would not be used for a permissible purpose.[79] These violations of the FCRA are considered unfair or deceptive acts per se.[80]

<28>Lastly, the complaint alleged these failures to employ reasonable security measures rendered ChoicePoint's privacy statements false or misleading under Section 5. This is the same standard the FTC has applied in other

complaints involving privacy statements.[81]

COMMON FACTORS CITED BY THE FTC COMPLAINTS FOR BUSINESSES THAT FAIL TO EMPLOY REASONABLE SECURITY MEASURES UNDER SECTION 5

<29>When the FTC has brought Section 5 claims against businesses for failure to employ reasonable security measures, the FTC has noted a number of practices that, "taken together," failed to provide reasonable and appropriate security for personal information.[82] Such business practices can include:

- Not adequately assessing the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks.[83]
- Not implementing simple, low-cost, and readily available defenses to such attacks.[84]
- Failing to use strong passwords to prevent a hacker.[85]
- Storing the information in unencrypted files that could be accessed easily by using a commonly known user ID and password.[86]
- Failing to employ sufficient measures to detect unauthorized access.[87]
- Not encrypting the information while in transit or when stored on the in-store computer networks.[88]
- Using a commonly known default user id and password to protect consumer information.[89]

<30>The FTC has typically cited five or more of these and other factors when delineating the reasons a particular business failed to employ reasonable and appropriate security measures to protect personal information.[90]

COMMON REMEDIES INCLUDED IN SETTLEMENT AGREEMENTS FOR ALLEGED FAILURES TO IMPLEMENT APPROPRIATE SECURITY MEASURES UNDER SECTION 5

<31>Businesses that allegedly violated Section 5 because they failed to provide appropriate security for consumers' information, such as DSW and BJ's, have all entered into settlement agreements with the FTC.[91] While the settlements are not an admission of any violation,[92] the agreements do carry long term obligations for the businesses. Typically, the settlement agreements do not include any monetary penalties.[93] Commentators have noted that the agreements are "nearly uniform."[94]

<32>The settlement agreements have generally provided that the business must implement a comprehensive security program to protect consumer information. Typically, the programs must continue for 20 years.[95] The businesses must designate at least one employee to be accountable for the security program.[96] Specifically, the security programs must be "reasonably designed" to protect consumer information;[97] must proactively identify risks

and assess safeguards;[98] must be comprehensive of all aspects of the business;[99] and there must be regular testing or monitoring of the safeguards in place.[100] The businesses must also provide extensive reports and fund third-party audits of the program, typically for 10 to 20 years.[101]

<33>Some commentators[102] point out that the settlement agreements require measures nearly identical to those required under the Safeguards Rule,[103] which implements the Gramm-Leach-Bliley Act and which requires financial institutions to maintain a comprehensive security program to protect customer information.[104]

THE CHOICEPOINT SETTLEMENT CONTAINS HARSHER PENALTIES BECAUSE IT INVOLVED MORE SENSITIVE INFORMATION AND ALLEGED FCRA VIOLATIONS

<34>The settlement between ChoicePoint and the FTC has many similarities with settlements of cases involving only Section 5 violations such as BJ's, Guidance, and Cardsystems.[105] However, because of the alleged FCRA violations, ChoicePoint also agreed to pay $10 million in civil penalties and $5 million to redress consumers who were victimized by identity thieves using information released by ChoicePoint.[106]

<35>The $15 million ChoicePoint agreed to may be significantly lower than the fines they faced. Each violation of the FCRA carries civil penalties of up to $2,500.[107] A total of 163,000 records were alleged to have been sold to unauthorized buyers.[108] If each record was counted as a separate violation and the maximum penalty was imposed, the civil penalty would be as high as $407.5 million.

<36>Additionally, the ChoicePoint settlement includes other restrictive provisions that are different from the settlement agreements with businesses such as BJ's, Guidance, and Cardsystems. A unique feature of the ChoicePoint settlement is the compliance monitoring agreement. ChoicePoint authorized the FTC to secretly pose as ChoicePoint customers or employees to ensure compliance to the terms of the settlement.[109] The FTC may also interview any ChoicePoint employees or contractors and may obtain discovery from ChoicePoint.[110] None of this potentially invasive compliance monitoring is part of the typical FTC settlements for alleged Section 5 violations, such as those with Guidance and BJ's.

<37>The ChoicePoint settlement permanently bars future violations of the FCRA and FCTA. This is also unlike other FTC settlements such as those with BJ's and Guidance.[111] In those settlements, future violations of Section 5 would not explicitly be a breach of the agreement.[112]

STEPS BUSINESSES MAY TAKE TO AVOID AN FTC COMPLAINT FOR FAILING TO IMPLEMENT APPROPRIATE SECURITY MEASURES

<38>The two times the FTC has filed consumer information security related complaints against companies without actual security breaches have been when privacy promises were highly inconsistent with their actual practices[113] or when a breach was inevitable.[114] The remaining complaints have all been in response to an actual security breach.

<39>Businesses should respond quickly to address any security problems once they have been identified. The FTC has closed investigations of businesses believed to be violating their own privacy statements when those businesses acted quickly to improve their practices or improve the accuracy of their privacy statements.[115]

<40>One commentator believes that FTC statements indicate that, to prevent liability, companies should avoid the following security shortcomings: easy network access; lack of breach detection measures; unnecessary storage of consumer information; weak encryption or passwords; and inadequate defenses to known attacks.[116] Companies should therefore install robust security software, limit data storage and network access, and stay informed about well-known hacking techniques.[117] Further, companies could employ measures that the FTC has required in the consent agreements, such as having a designated employee responsible for security and privacy protection.[118]

<41>When considering security measures, it is also important to consider the type of information being protected. FTC complaints have all cited a failure to employ appropriate security measures. In this context, “appropriate” includes the duty to have a level of security commensurate with the sensitivity of consumer information. Particularly sensitive information includes debit and credit card information or other information that can be used to commit fraud. Sensitive information also includes Social Security numbers and dates of birth because they may be used to commit identity theft.[119]

<42>**Chronological Table of Security Breach FTC Settlements**[120]

Party	**Type of information**	**Type of security threat**	**Actual breach**	**Privacy policy violated**	**Third party accessing information**	**Additional issues**	**Year**[1]
Eli Lilly	Email addresses	Unclear	Yes	Yes	Accidentally, other customers		2002
Microsoft	Credit card numbers, addresses	Credit card fraud	No	Yes	None occurred, criminals could have	Children’s and adult’s info	2002
Guess	Credit card numbers	Credit card fraud	Yes	Yes	“Hackers”		2003
Tower Records	Address, email, phone, name, past purchases	Identity theft (maybe)	Unclear	Yes	Unclear		2004

Petco	Credit card numbers	Credit card fraud	Yes	Yes	“Hacker”		2004
BJ’s Wholesale	Name, credit and debit card number, expiration date	Credit and debit card fraud	Yes	No policy	Criminals committing fraud	Millions of dollars of fraudulent purchases	2005
Choice-Point	Names, social security numbers, DOB, credit histories	Identity Theft, leading to fraud	Yes – info was sold to criminals	Yes	Criminals committing fraud and identity theft	$15 million in fines to ChoicePoint. Had poor screening system.	2006
Card-Systems	All credit and debit card security info of customers	Credit and debit card fraud	Yes	No policy	Criminals committing fraud	Resulted in millions of dollars in fraud	2006
DSW	Credit card, debit card, checking account information	Fraud	Yes	No policy	Criminals committing fraud - “hackers”	1.4 million customers information was accessed	2005
Guidance	Credit card information	Credit card fraud	Yes	Yes	Criminals committing fraud - “hackers”	Thousands of customers’ information was accessed	2006
Life is good	Credit card information		Yes	Yes	“Hackers”	Thousands of customers’ information was accessed	2008
Goal Financial	Information from student loan applications	Unclear	Sold and transferred info to un-authorized	Yes	Unauthorized individuals	Safeguard Rule and Privacy Rule, which	2008

			parties			implement the GLBA, allegedly violated	
Reed Elsevier and Seisint	Social security numbers, DOB, addresses, and other personal information	Identity theft and fraud	Yes	No	"Identity thieves"	Hundreds of thousands of LexisNexis customers' information stolen	2008
TJX	Debit and credit card information, other personal information	Credit and debit card fraud	Yes	No	"An intruder… installed hacker tools"	Breach resulted in tens of millions of dollars of fraudulent charges	2008

CONCLUSION

<43>Businesses dealing with and storing consumer information should be diligent in employing reasonable security measures that are appropriate given the sensitivity of the information. The FTC's decision to expand the breadth of its complaints by including businesses without any privacy promises reveals its aggressive posture. Now all businesses subject to the FTCA may be held accountable for protecting sensitive consumer information. It appears the FTC has adopted the responsibility to police information security in response to the void of any common law or explicit statutory remedies against businesses that neglect to protect consumers. Given the FTC's significant discretion in determining what constitutes unfair or deceptive trade practices, the FTC may choose to file future complaints against businesses for less egregious security failures than those alleged at BJ's and Choicepoint.

PRACTICE POINTERS

- Practitioners should inform businesses that the FTC may impose civil penalties against businesses that are robbed by thieves stealing sensitive consumer information such as Social Security numbers, dates of birth, bank and credit card account information, and credit histories.
- If a business is attacked by hackers or other kinds of thieves stealing sensitive consumer information, the FTC may not take action against the business if it finds that the business has employed reasonable and appropriate measures to secure the personal information of its customers. Such measures include adequate security software, protections against well-known hacking methods, limiting the time personal information is stored,

limiting access to networks, and having a method of detecting and investigating unauthorized access. Further, businesses should take precautions against the threat of insider theft of consumer information.

- Businesses should also be aware that their privacy statements may establish additional duties, such as the duty not to share consumers' personal information with other parties. Businesses must be sure that their practices are consistent with their statements on privacy and security.
- Be aware that state security laws such as California AB 1950, breach notification laws, and state and federal privacy laws may impose additional security requirements for your clients' businesses.

<< Top

Footnotes

1. Joel B. Hanson, University of Washington School of Law, Class of 2008. Thank you to Professor Anita Ramasastry, University of Washington School of Law; Chris Hoofnagle, Berkeley Center for Law & Technology; Laura Dunlop; Suzanna Storment; and Jen Chiang.
2. *See* Jay Cline, *Lessons Learned from Corporate Security Breaches*, COMPUTERWORLD, Aug. 9, 2005, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,103733,00.h .
3. *See id.* Half of the reported breaches in the survey were due to "external hackers."
4. *See id.*
5. *See* Jonathan Krim, *LexisNexis Data Breach Bigger Than Estimated*, WASHINGTON POST, Apr. 13, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A45756-2005Apr12.html.
6. Antony Savaas, *TJX hack the biggest in history*, COMPUTERWEEKLY.COM, Apr. 2, 2007, *available at* http://www.computerweekly.com/Articles/2007/04/02/222827/tjx-hack-the-biggest-in-history.htm.
7. *Id. See also* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FEDERAL LAWYER, Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw). *See generally* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP (last visited May 8, 2007).
8. *See* Evan Schuman, *The Meaning of TJX's $168 Million Data Breach Cost*, EWEEK.COM, Aug. 15, 2007, http://www.eweek.com/article2/0,1895,2171101,00.asp. TJX estimates that investigating these breaches and defending against all related litigation may eventually cost as much as $168 million.

9. *See* Complaint, In the Matter of TJK Companies, Inc. (FTC 2008), *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf; Agreement Containing Consent Order, In the Matter of TJK Companies, Inc., No. 072 3055 (FTC 2008), *available at* http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf; Complaint, In the Matter of Reed Elsevier Inc. and Seisint, Inc. (FTC 2008), *available at* http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf; and Agreement Containing Consent Order, In the Matter of Reed Elsevier Inc. and Seisint, Inc., No. 0523094 (FTC 2008), *available at* http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.

10. 15 U.S.C. § 45(a)(1) (2007). "Section 5" refers to the section of the public law that prohibits unfair or deceptive trade practices.

11. The FTC has broad authority to determine what trade practices are unfair or deceptive. *See, e.g.,* E. I. Du Pont de Nemours & Co. v. FTC, 729 F.2d 128, 136 (2d Cir. 1984) ("Congress sought to provide broad and flexible authority to the Commission … The specific practices that might be barred were left to be defined by the Commission, applying its expertise, subject to judicial review . . . [I]ts interpretation of § 5 is entitled to great weight, and its power to declare trade practices unfair is broad"); American Financial Services Ass'n. v. FTC, 767 F.2d 957, 966 (D.C. Cir. 1985) ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field . . . Whether competition is unfair or not generally depends upon the surrounding circumstances of the particular case."), *cert. denied*, 475 U.S. 1011 (1986). *See also* 54A Am. Jur. 2d *Monopolies and Restraints of Trade* § 1154 (2007).

12. "An account level breach involves mostly account data such as credit card numbers and credit card expiration dates." *Financial Data Protection Act of 2005: Hearing on H.R. 3997 Before the Subcommittee on Financial Institutions and Consumer Credit*, 109th Cong. 2 (2005) (written submission of data breach research by ID Analytics Corporation), *available at* http://financialservices.house.gov/media/pdf/110905ida.pdf.

13. 15 U.S.C. § 1681 et seq. (2007).

14. *Id.* "An identity level breach involves the most sensitive data available – names, Social Security Numbers (SSNs), dates of birth, addresses, and other personally-identifiable information."

15. *See, e.g.,* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L.J. 1553 (2005); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255 (2005); Kimberly Kiefer & Randy V. Sabett, *Openness of Internet Creates Potential for Corporate Information Security Liability*, 7 BNA ECLR 594 (2002); Erin Kenneally, *Stepping on the Digital Scale: Duty and Liability for Negligent Internet Security*, ;login: The USENIX Magazine, Dec. 2001, *available at* http://www.usenix.org/publications/login/2001-

12/pdfs/kenneally.pdf.

16. Courts have been reluctant to find injuries in fact, proof of damages, or grant standing when consumer information has been stolen. *See* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FEDERAL LAWYER, Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw). . *See also* Denis T. Rice, *Increased Civil Litigation Over Privacy and Security Breaches*, 902 PLI/PAT 149 (2007); Kirk J. Nahra, *What Every Litigator Needs to Know About Privacy*, 902 PLI/PAT 277 (2007); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 519 (2006) (noting that "courts are reluctant to find harm simply from the insecure storage of information."). *But cf.* Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874 (W.D. Tenn. 2007) (holding that bank had common law duty to verify the authenticity and accuracy of a credit account application before issuing a credit card and allowing negligence claim against bank).

17. *See* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206 (M.D. Pa. 2006) (granting summary judgment to defendant where debit card issuer sued BJ's for losses resulting from the fraudulent use of cards as a result of the BJ's security breach); Sovereign Bank v. BJ's Wholesale Club, Inc., 427 F.Supp.2d 526, 533 (M.D. Pa. 2006) (dismissing negligence claim against BJ's by another debit card issuer suing for losses incurred from the fraudulent use of cards resulting from the BJ's security breach); Pennsylvania State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317 (M.D. Pa. 2005) (dismissing claims by credit union against BJ's and against IBM which provided software used by BJ's for their transactions). *See also* Parke v. CardSystems Solutions, Inc., No. C 06-04857 WHA, 2006 WL 2917604 (N.D. Cal. 2006) (plaintiffs attempting class action suit for consumers affected by security breach).

18. *See, e.g.,* Bell v. Michigan Council 25, No. 246684, 2005 WL 356306 (Mich. App. Feb. 15, 2005), *cert denied*, 707 N.W.2d 597 (Mich. Dec 28, 2005) (finding liability for union's breach of a duty to protect personal information "based on ordinary negligence principles"); Guin v. Brazos Higher Educ. Serv., 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006) (stating that "in some negligence cases . . . a duty of care may be established by statute" and applying the Gramm-Leach-Bliley Act to establish the duty of care, but holding that there was not a breach of that duty in the case).

19. To date, TJX has paid $65 million to settle lawsuits. Ross Kerber, *TJX settles with MasterCard over data breach*, THE BOSTON GLOBE, Apr. 2, 2008, *available at* http://www.boston.com/business/ticker/2008/04/tjx_settles_wit_1.html .

20. *See* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FEDERAL LAWYER, Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw).

21. The Federal Trade Commission Act ("FTCA") established the FTC in 1914. Passed in 1938, the Wheeler-Lea Amendment prohibits

"unfair or deceptive acts or practices." The FTC enforces this law and, through the Magnuson-Moss Act of 1975, may adopt rules that more explicitly define unfair and deceptive acts or practices.

22. 15 U.S.C. § 45(a)(1) (2007).

23. 15 U.S.C. § 45(n) (2007).

24. *See* Complaint, In the Matter of Geocities, No. C-3850 (FTC 1999), *available at* http://www.ftc.gov/os/1999/02/9823015cmp.htm.

25. This violation of a privacy policy was alleged to be "unfair or deceptive acts or practices." The FTC did not specify whether it was unfair or deceptive. *See* Complaint at 4, In the Matter of Petco Animal Supplies, Inc. (FTC 2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf.

26. For a complete list of all FTC privacy complaints and settlement agreements, *see* FTC, Privacy Initiatives, Unfairness and Deception, Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited May 5, 2008).

27. *See* Complaint, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

28. *Id*. at 2.

29. *See, e.g.*, Complaint at 3, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

30. Deceptive acts or practices should not be conflated with unfair acts or practices. Deceptive acts are those that involve false or misleading information. On the other hand, labeling certain acts as unfair effectively sets a normative baseline for business practices. The FTC is cautious with its authority to determine that acts are unfair, because this may have the effect of banning business models in the interest of protecting consumers.

31. Complaint, In the Matter of DSW Inc., No. C-4157 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf ; Complaint, In the Matter of Cardsystems, Inc. (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf.

32. Complaint, In the Matter of DSW Inc., No. C-4157 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf ; Complaint, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf ; Complaint, In the Matter of Cardsystems, Inc. (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf.

33. *See* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FEDERAL LAWYER, Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw).

34. *See* 15 U.S.C. § 45(n) (2007). Unfair or deceptive trade practices are limited to only those practices that cause or are likely to cause substantial injury to consumers which are not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

35. *See, e.g.,* E. I. Du Pont de Nemours & Co. v. FTC, 729 F.2d 128, 136 (2d Cir. 1984) (stating that Congress intended the FTC to have broad and flexible authority to declare what trade practices are unfair); Am. Fin. Servs. Asso. v. FTC, 767 F.2d 957, 966 (D.C. Cir. 1985) ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. . . . Whether competition is unfair or not generally depends upon the surrounding circumstances of the particular case."), *cert. denied*, 475 U.S. 1011 (1986). *See also* 54A AM. JUR. 2d *Monopolies and Restraints of Trade* § 1154 (2007).

36. *See* Donald M. Zupanec, Annotation, *Practices Forbidden by State Deceptive Trade Practice and Consumer Protection Acts*, 89 A.L.R.3d 449, § 2(b) (2007).

37. *See, e.g.* Complaint, In the Matter of Vision I Props., LLC, d/b/a CartManager Int'l. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423068/050310comp0423068.pdf (allegedly renting out the personal information of one million customers for marketing purposes was a violation of privacy statement).

38. *See, e.g.* Complaint, In the Matter of Petco Animal Supplies, Inc. (FTC 2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf.

39. Complaint at 4-5, In the Matter of Microsoft Corporation, No. C-4069 (FTC 2002), *available at* http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf (promising parents of child users a level of control and security benefits that did not in fact exist).

40. Complaint at 3, In the Matter of MTS, Inc., and d/b/s Tower Records (FTC 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040421comp0323209.pdf (customers' personal information was easily accessible on company's website and was viewed by other customers despite statement to the contrary in company's privacy policy).

41. As of February 20, 2008, the Life is good, Inc. complaint and subsequent settlement is the most recent example of the FTC alleging a business has violated its privacy policy by failing to implement reasonable security measures. Complaint, In the Matter of Life is good, Inc. (FTC 2008), *available at* http://www.ftc.gov/os/caselist/0723046/080117complaint.pdf.

42. Complaint at 1, In the Matter of Petco Animal Supplies, Inc. (FTC

2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf.

43. *Id.* at 2.

44. *Id.* at 3.

45. *Id.*

46. *Id.* at 4.

47. *Id.*

48. Press Release, FTC, Petco Settles FTC Charges (Nov. 17, 2004), *available at* http://www.ftc.gov/opa/2004/11/petco.shtm.

49. Complaint at 2, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

50. *See id.* at 3; Complaint at 3, In the Matter of Cardsystems, Inc. (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf; Complaint at 3, In the Matter of DSW Inc., No. C-4157 (FTC Mar. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf .

51. *See id*.

52. *See id.*

53. Complaint at 2, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

54. *Id*.

55. *Id*.

56. *Id.*

57. *Id.*

58. *Id.* at 2-3.

59. *Id.* at 3.

60. Complaint at 1, In the Matter of Cardsystems, Inc. (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf.

61. *Id.* at 1-2.

62. *Id.* at 2.

63. *Id*.

64. *Id*.

65. *Id.*

66. Cardsystems created unnecessary risks to the information by storing it in a vulnerable format for up to 30 days; did not use

readily available security measures to limit access between computers on its network and between such computers and the Internet; and failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations. *Id*.

67. Complaint at 2, In the Matter of Cardsystems, Inc. (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf.

68. *Id.*

69. Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

70. The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. 15 U.S C. § 1681a(f) (2007).

71. Complaint at 4, U.S. v. Choicepoint Inc., No. 106-CV-0198 (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

72. *Id.*

73. *Id.*

74. *Id* at 4-7.

75. *Id.*

76. *Id.*

77. *Id.*

78. A violation under 15 U.S C. § 1681c(a) (2006). Complaint at 7, U.S. v. Choicepoint Inc., No. 106-CV-0198 (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

79. A violation under 15 U.S.C. § 1681e(a) (2006). Complaint at 8, U.S. v. Choicepoint Inc., No. 106-CV-0198 (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

80. A violation under 15 U.S.C. § 1681s(a)(1) (2006). Complaint at 8, U.S. v. Choicepoint Inc., No. 106-CV-0198 (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

81. *See, e.g.* Complaint, In the Matter of Petco Animal Supplies, Inc. (FTC 2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf ; Complaint, In the Matter of Guidance Software, Inc. (FTC 2006),

available at http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20complaint.pdf.

82. *See, e.g.* Complaint at 2, In the Matter of DSW Inc., No. C-4157 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf .

83. Complaint at 2, In the Matter of Cardsystems, Inc. (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf.

84. *Id.*

85. *Id.*

86. Complaint at 2, In the Matter of DSW Inc., No. C-4157 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf .

87. *Id*.

88. Complaint at 2, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.

89. *Id.*

90. *See, e.g.,* Complaint at 2, In the Matter of BJ's Wholesale Club, Inc. (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf ; Complaint at 2, In the Matter of DSW Inc., No. C-4157 (FTC Mar. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf .

91. *See, e.g.,* Agreement Containing Consent Order, In the Matter of DSW, Inc., No. 052-3096 (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0523096/051201agree0523096.pdf .

92. *See, e.g., id*. at 2.

93. *See, e.g. id.*; Agreement Containing Consent Order, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf.

94. Rebecca S. Eisner, *Securing Private Information in Service Provider Arrangements: New Developments Shape Emerging U.S. Privacy Standards*, 913 PLI/PAT 11 (2007).

95. The 20 year period for the settlement is restarted if the FTC ever files another complaint that is not dismissed. *See, e.g.,* Agreement Containing Consent Order at 6, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing

Consent Order at 6, In the Matter of BJ's Wholesale Club, Inc., No. 0423160 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf .

96. *See, e.g.*, Agreement Containing Consent Order at 3, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing Consent Order at 3, In the Matter of CardSystems Solutions, Inc., No. 0523148 (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf.

97. *See, e.g.*, *id*.

98. *See, e.g.* Agreement Containing Consent Order at 3-4, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing Consent Order at 3-4, In the Matter of CardSystems Solutions, Inc., No. 0523148 (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf.

99. *See, e.g.*, Agreement Containing Consent Order at 3, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing Consent Order at 3-4, In the Matter of CardSystems Solutions, Inc., No. 0523148 (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf.

100. *See, e.g.*, Agreement Containing Consent Order at 4, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing Consent Order at 4, In the Matter of CardSystems Solutions, Inc., No. 0523148 (FTC 2005), *available at* http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf.

101. *See, e.g.*, *id*.

102. Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, FEDERAL LAWYER, Sept. 2007, at 39, *available at* 54-SEP Fed. Law. 39 (Westlaw) (arguing that the FTC is effectively expanding the Safeguards Rule to retail businesses by imposing such terms in the settlement agreements).

103. 16 C.F.R. § 314. *See also* FTC, Safeguards Rule: Laws and Rules, http://www.ftc.gov/privacy/privacyinitiatives/safeguards_lr.html (last visited May 5, 2008).

104. 15 U.S.C. § 6801(b) (2007) ("each financial institution has an affirmative and continuing obligation to respect the privacy of its

customers and to protect the security and confidentiality of those customers' nonpublic personal information").

105. The settlement requires a permanent implementation of a comprehensive security program. Stipulated Final Judgment and Order of Civil Penalties, Permanent Injunction, and Other Equitable Relief at 14, U.S. v. Choicepoint Inc. (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf. This permanent program is in contrast to the 20 years typically required in the other FTC settlements. As in other FTC settlements, the program must be reasonably designed to protect consumer information. *Id*. Also as in other FTC settlements, one or more employees must be accountable for the security program, there must be risk assessment, and there must be testing and monitoring. *Id*. at 15. Like the Guidance settlement, ChoicePoint must have an independent audit of its security every 20 years. *Id*. at 16.

106. Press Release, FTC, FTC Launches Redress Program for ChoicePoint Identity Theft Victims (December 6, 2006), *available at* http://www.ftc.gov/opa/2006/12/choicepoint.shtm. The FTC contacted 1,400 individuals that it believes may have been victims of identity theft as a result of the alleged violations by ChoicePoint.

107. 15 U.S.C. § 1681s(a)(2)(A) (2007).

108. Complaint at 4, U.S. v. Choicepoint Inc., No. 106-CV-0198 (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

109. Stipulated Final Judgment and Order of Civil Penalties, Permanent Injunction, and Other Equitable Relief at 18-19, United States of America v. Choicepoint Inc. (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

110. *Id.*

111. *See, e.g.*, Agreement Containing Consent Order, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing Consent Order, In the Matter of BJ's Wholesale Club, Inc., No. 0423160 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf .

112. Note, however, that such settlements will restart the 20 year period of the security program requirement if the FTC later files a complaint that is not dismissed. So a violation of the FCTA, or even an alleged violation, would still have repercussions. Agreement Containing Consent Order, In the Matter of Guidance Software, Inc., No. 062-3057 (FTC 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Agreement Containing Consent Order, In the Matter of BJ's Wholesale Club, Inc., No. 0423160 (FTC 2006), *available at*

http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf .

113. Complaint at 4-5, In the Matter of Microsoft Corporation, No. C-4069 (FTC Dec. 20, 2002) (promising parents of child users a level of control and security benefits that did not in fact exist), *available at* http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

114. Complaint at 3, In the Matter of MTS, Inc., and d/b/s Tower Records (FTC 2004) (customers' personal information was easily accessible on company's website and was viewed by other customers in spite of privacy promise), *available at* http://www.ftc.gov/os/caselist/0323209/040421comp0323209.pdf.

115. *See, e.g.*, Letter from Mary Koelbel Engle, Associate Director, Division of Advertising Practices, FTC, to Thomas M. Hughes, Hunton & Williams (May 31, 2002), *available at* http://www.ftc.gov/os/closings/staff/earthlinkclose.shtm (Re: EarthLink, Inc., Matter No. 002 3258); Letter from C. Lee Peeler, Associate Director, Division of Advertising Practices, FTC, to Susan P. Crawford, Wilmer, Cutler & Pickering (Nov. 17, 2000), *available at* http://www.ftc.gov/os/closings/staff/yahooinc.pdf (Re: Yahoo! Inc.).

116. Rebecca S. Eisner, *Securing Private Information in Service Provider Arrangements: New Developments Shape Emerging U.S. Privacy Standards*, 913 PLI/PAT 11 (2007).

117. *Id.* at 29-30.

118. *Id.* at 31-33.

119. Complaint at 4, U.S. v. Choicepoint Inc., No. 106-CV-0198 (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

120. All the information in this table is based upon complaints, press releases, and other documents from the FTC website. FTC, Privacy Initiatives, Unfairness and Deception, Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Mar. 10, 2008).

121. This field indicates the year of the settlement agreement. Where there were multiple agreements, the year corresponds to the date of the initial settlement agreement.