PrivacyStudio.com
The Art of Information Management

THE PRIVACY CASE BOOK:

A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks

CHAPTER 4
Information Security

Margaret P. Eisenhauer, Esq., CIPP
Privacy and Information Management Services – Margaret P. Eisenhauer, P.C.

Chapter Four
INFORMATION SECURITY

Probably no fact patterns have generated as much enforcement activity in recent years as security incidents. Regulators worldwide expect companies that handle sensitive personal information to have reasonable measures in place to protect that information. While regulators realize that security programs are not perfect and incidents happen to all companies, they are quick to use their enforcement powers to address perceived weaknesses in security programs.

Security Requirements for Regulated Entities

Companies in regulated industries, such as financial services and healthcare, are generally subject to statutory security program requirements. In the United States, the most obvious of these are the Safeguards Rule promulgated by the Federal Trade Commission and Federal financial institution regulators under **the Financial Services Modernization Act of 1998 (a.k.a. The Gramm-Leach-Bliley Act)**,[73] and the Security Rule promulgated by the Department of Health and Human Services (HHS) under **The Health Insurance Portability and Accountability Act of 1999 (HIPAA)**.[74] Outside the United States, functional regulators promulgate similar rules for their regulated entities. Companies violate these rules at their peril.

THE NATIONWIDE BUILDING SOCIETY CASE (FEBRUARY 2007)[75]

Respondent: Nationwide Building Society

Regulator: Financial Services Authority (FSA) – a UK Functional Regulator

Basis for Complaint: Violation of Financial Services and Markets Act 2000 (FSMA)

Facts and Allegations: Respondent is a UK-based financial institution. It is the largest building society in the world, offering mortgages, savings and other financial services to over eleven million customers.

Section 2(2) of the FSMA requires regulated entities to undertake (as an objective) "Reducing the extent to which it is possible for a business carried on by a regulated person …to be used for a purpose connected with a financial crime."

Principle 3 of the FSA's Principles for Businesses requires that every regulated entity "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems." Additionally, in 2004, the FSA published an Information Security Report to raise awareness of the risks of financial crimes and to encourage action to reduce risk. The FSA has undertaken numerous initiatives to increase awareness of the issues around information security and the risks of identity theft.

In August 2006, a laptop containing Nationwide's confidential customer information was stolen from the home of an employee. The information could be used to further financial crimes.

The FSA's investigation revealed that, while Nationwide had taken some steps to improve its security, it had failed to take adequate steps to reduce the risk of loss of customer information. The information security procedures it had in place were housed electronically in multiple documents that were difficult to find or apply to particular roles. In addition, the policies contained inconsistencies and lacked both prioritization of issues and clarity between mandatory requirements and best practices. The staff received only generic training on these procedures and could simply self-certify that they had read and understood the procedures.

The FSA alleged that Nationwide was slow to investigate the information contained on the stolen laptop due to inadequate incident management procedures, thereby increasing the opportunity for the stolen information to be used in financial crime.

The FSA also alleged that Nationwide failed to establish appropriate controls and monitoring mechanisms to mitigate risk of such an incident by failing to adequately:

- Assess the risks in relation to the security of customer information;
- Manage the risks it faced with its existing information security procedures;
- Implement training and monitoring with its staff;
- Implement controls to mitigate information security risks, ensure that employees understood and followed procedures, and ensure that an appropriate level of information security was provided; and
- Implement appropriate procedures to deal with an incident involving exposure of customer information.

Outcome: The FSA entered into a Final Notice with Nationwide imposing a fine. During the investing, Nationwide took steps to address the security program deficiencies. The FSA noted that Nationwide has chosen to address the risks to its customers by:

(a) Taking additional measures to increase its security;

(b) Informing its customers in writing of the loss of information and steps they can take to minimize their risk of identity theft;

(c) Affirming its existing policy of reimbursing customers for financial loss suffered as a result of the incident; and

(d) Hiring an independent third party to perform a comprehensive review of its information security procedures and controls.

Fine Imposed: £980,000 (Note that this fine reflects a 30% reduction in the proposed fine due to Nationwide's acceptance of the order during an executive settlement proceeding. The proposed FSA fine was £1,400,000.)

The FSA continues to take action against regulated companies that do not appropriately protect sensitive customer information. In December 2007, it imposed a record fine of £1.26 million on Norwich Union Life, the largest United Kingdom life insurance business, based on its failure to address

a pattern of unauthorized access to customer policy information by fraudsters via the company call center.[76]

THE SUPERIOR MORTGAGE CASE (DECEMBER 2005)

Respondent: Superior Mortgage Corporation

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Gramm-Leach-Bliley Safeguards Rule

Facts and Allegations: Respondent is a direct lender, specializing in residential mortgage loans. It is a New Jersey corporation with offices located in ten different states. During the mortgage application process, Superior Mortgage collects personal information (Social Security numbers, credit histories, and bank and credit card numbers) through its branch offices and through its six websites.

The FTC complaint alleged that Superior Mortgage failed to implement reasonable security policies and procedures as required by the Gramm-Leach-Bliley Safeguards Rule.

Between May 2003 and at least May 2005, Superior Mortgage allegedly failed to do the following:

- Conduct timely risk assessments of its customer information;
- Control access to customers' personal information through use of password policies;
- Encrypt the personal information of its customers' that was emailed using outside computer networks; and
- Oversee its service providers to ensure that appropriate security was being used to protect its customers' information.

In addition, through its website, Superior Mortgage made false and misleading representations to consumers regarding the privacy and security of the personal information collected.

Outcome: The FTC entered into a consent decree with Superior Mortgage, ordering:

Bar on Misrepresentation: Superior Mortgage shall not misrepresent the extent to which consumers' personal information is protected by SSL encryption, or the extent to which it maintains and protects the privacy or confidentiality of the collected personal information.

Security Program: [Required under the GLBA Safeguards Rule]

Third Party Audit: Within 180 days after service of order and thereafter biannually for ten years, Superior Mortgage must obtain an assessment and report from an independent, third party that:

(1) Sets forth the specific safeguards implemented and maintained by Superior Mortgage;

(2) Explains how such safeguards are appropriate for the size and complexity of Superior Mortgage, the nature and scope of Superior Mortgage's activities and the sensitivity of the consumers' information;

(3) Explains how the implemented safeguards meet or exceed the protections required by the Safeguards Rule; and

(4) Certifies that Superior Mortgage's security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

Maintenance of Relevant Documents:

(1) Superior Mortgage shall maintain and provide to the FTC the initial Assessment and all materials relied upon to prepare the assessment within ten days after the first assessment; and

(2) For a period of three years after each biennial assessment, Superior Mortgage must retain a copy of each such assessment and all materials relied upon in preparing the assessment, and, upon request, provide all information within ten days of request.

Delivery of Order: Superior Mortgage shall deliver a copy of the FTC order to all current and future principals, officers, directors, and managers and to all current and future employees, agents and representatives with supervisory responsibility over the subject matter.

Reporting: Superior Mortgage shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Within 180 days after service of order and thereafter as requested, Superior Mortgage shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None

Regulated entities in other countries have faced sanctions for inadequate security as well. In Japan, the Financial Services Agency ordered Michinoku Bank Ltd. to improve security processes in May 2005, after the bank lost three CD-ROM discs containing account holder information.[77] This was the first enforcement action conducted by the FSA, after the Japanese Personal Information Protection Law took effect.

Similarly, the Canadian Privacy Commissioner has addressed security issues related to the misdirection of faxes by banks, ordering additional controls.[78] The French data protection authority has fined financial institutions for inadequate controls, including failure to properly manage bad credit lists. These sanctions included a €45,000 fine against Credit Lyonnais, a €20,000 fine against Credit Argicole, and a €30,000 fine against Banque des Antilles Francaises.[79]

General Security Requirements under International Data Protection Laws

Appropriate security for personal information is a fundamental requirement of data protection theory. The 1980 OECD Privacy Guidelines, which represented the first major international consensus on privacy principles, included the Security Safeguards Principle:[80]

> *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

Similarly, the 2004 APEC Privacy Principles include Principle VII, Security Safeguards:[81]

> *Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.*

The commentary to the APEC Privacy Principles notes that "this Principle recognizes that individuals who entrust their information to another are entitled to expect that their information be protected with reasonable security safeguards."[82]

Simply put, companies have an obligation to provide reasonable security for personal information under virtually all privacy and data protection laws. To supplement this general obligation, many data protection laws (such as Australia, Canada and Hong Kong) include a requirement for appropriate security expressed in legally-binding data protection principles. Additionally, many data protection authorities have published mandatory security standards. For example, the data protection authorities of Greece, Spain, Poland, and Italy have issued various security requirements for companies subject to their data protection laws.

THE BANK BRIEFCASE CASE (2003)[83]

Respondent: A Bank

Regulator: Privacy Commissioner for Personal Data ("PCPD")

Basis for Complaint: Violation of Data Protection Principle 4 ("DPP4") of the Hong Kong Personal Data (Privacy) Ordinance

Facts and Allegations: The Bank conducted a marketing campaign in a bookstore to solicit credit card applications. At the end of the day, a bank employee put the application forms along with copies of applicants' national identity cards in a briefcase to carry them home. The employee accidentally left the briefcase on a public bus, losing all the documents.

DPP4 states: "Security of personal data – This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable)." The PCPD determined that the bank did not have adequate guidelines for information security and had not adequately educated its staff regarding security, in violation of DPP4.

Outcome: The PCPD issued an enforcement notice against the bank. The bank agreed to implement appropriate security measures, including delivery of the credit card applications directly to the bank branch at the end of each campaign day.

Fine Imposed: None

THE INSURANCE INFORMATION CASE (APRIL 2007)[84]

Respondent: An Australian insurance company

Regulator: Office of the Privacy Commissioner (Australia)

Basis for Complaint: Violation of the National Privacy Principles in Schedule 3 of the Privacy Act 1988

Facts and Allegations: A complaint was filed with the Privacy Commissioner's Office against an insurance company based on disclosure of the person's account information to an unauthorized third party. The individual discovered that his account information had been included on account statements provided to a third party for the previous two years. The individual was not satisfied with the insurance company's response to the situation. He also expressed general concerns about the accuracy and security of his information and the privacy practices of the insurance company.

The Commissioner's Office noted that:

- National Privacy Principle 2.1 provides that personal information collected for a primary purpose may only be used or disclosed for a secondary purpose if one of a number of exceptions in National Privacy Principle 2.1(a)-(h) apply;

- National Privacy Principle 3 provides that an organisation must take reasonable steps to ensure that the personal information it collects uses or discloses is accurate, complete and up to date; and

- National Privacy Principle 4.1 provides that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

Outcome: The Privacy Commissioner conducted preliminary enquiries and also referred the complaint to the insurance company in order for it to further consider the issues raised by the complainant before the commencement of a formal investigation. In response, the insurance company advised that it had counseled the particular staff members involved on the issues and circulated a notice to all its call centers and branches reminding staff of their obligations under the Privacy Act. The insurance company also agreed to consider the suggestions made by the complainant to further ensure the information was up to date, accurate and complete.

The insurance company also offered an apology to the complainant and a payment of A$1,250 in full settlement of the case. The complainant accepted the apology and payment, and the Commissioner deemed the matter resolved.

Fine Imposed: None (A voluntary payment of A$1,250 was made to claimant to settle case.)

THE TJX INVESTIGATION (SEPTEMBER 2007)[85]

Respondent: TJX Companies, Inc., Winners Merchant International L.P.

Regulators: Office of the Privacy Commissioner of Canada and the Office of the Privacy Commissioner of Alberta

Basis for Complaint: Violation of the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Personal Information Protection Act (PIPA), the Alberta provincial privacy law

Facts and Allegations: TJX discovered that a breach of its computer networks had exposed payment card data and other personal information of approximately 45 million individuals in Canada, the US, and other countries. As a result of this event, the Privacy Commissioner of Canada and the Privacy Commissioner of Alberta each launched an investigation to determine if TJX had violated their respective privacy laws. The Commissioners elected to combine efforts and conduct a joint investigation of the companies' data collection, retention and security practices. In particular, the Commissioners considered three questions:

(1) Did TJX have a reasonable purpose for collecting the personal information affected by the breach?

(2) Did TJX retain the personal information in compliance with PIPEDA and PIPA?

(3) Did TJX have reasonable safeguards in place to protection the personal information in its custody?

After the investigation, the Commissions concluded that TJX contravened various provisions of PIPEDA and PIPA in its data collection, retention and safeguarding practices. (Specifics of the violations are presented in detail in the published *Report of an Investigation into the Security, Collection and Retention of Personal Information*, TJX Companies Inc. /Winners Merchant International L.P., September 25, 2007.)

With regard to the third question, the Commissioners evaluated TJX's safeguards against Principle 4.7 of PIPEDA, which states that personal information shall be protected by security safeguards appropriate to the sensitivity of the information, and section 34 of PIPA, which states that an organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

PIPEDA Principle 4.7 provides additional guidance on the obligations:

- Principle 4.7.1 of PIPEDA stipulates that the security safeguards shall protect personal information against loss or threat, as well unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

- Principle 4.7.2 adds that the nature of the safeguards will vary depending on the nature of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.

- Under Principle 4.7.3, the methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption.

- Principle 4.7.4 notes that organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

- Principle 4.7.5 requires that care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

Accordingly, the Commissioners determined that TJX had a duty under PIPEDA and PIPA to safeguard personal information in its custody or under its control. In examining whether TJX's security measures constituted "reasonable security arrangements", the Commissioners considered whether TJX looked at its entire systems and fully assessed their vulnerabilities, taking into account the foreseeability of the security risk, the likelihood of damage occurring, the seriousness of the harm, the cost of preventative measures, and relevant standards of practice.

The Commissioners noted that, given the sensitivity of the personal information that was accessed by the intruders, the number of affected individuals, and the time that elapsed before the intrusion was detected, the harm caused could be quite serious. The perpetrator(s) had access to millions of credit card numbers for an extended period of time, long enough to commit credit-card fraud or to pass information on to others to do the same. Moreover, the breach exposes individuals to an increased level of anxiety as well as the costs associated with dealing with any actual fraud.

The Commissioners further noted that legislative requirements typically establish minimum standards for conduct. The fact that encryption is included as a safeguard under Principle 4.7.3 of PIPEDA suggests that it is an established measure of protection. Although TJX had an encryption protocol in place, it was a weak protocol (WEP) that was known to be easily defeated. Since 2003, experts had recommended moving from WEP to the more secure WPA protocol.

The Commissioners observed that the Payment Card Industry Data Security Standard (PCI DSS) version 1.1, was released September 2006 and required WPA technology. TJX should have been adhering to PCI DSS version 1.1. The breaches took place over a period of time and extended beyond the new PCI version.

Furthermore, while TJX took the steps to implement a higher level of encryption, the Commissioners determined that TJX did not segregate its data so that cardholder data could be held on a secure server while it undertook its conversion to WPA. Finally, although TJX had a duty to monitor its systems vigorously, it did not do so; if adequate monitoring of security threats had been in place, TJX should have been aware of an intrusion prior to December 2006.

The Commissioners concluded that the risk of a breach was foreseeable based on the amount of sensitive personal information retained and the fact that the weaknesses of WEP encryption were well known. Additionally, information should have been segregated and the systems better monitored. Therefore, TJX did not meet the safeguard provisions of either PIPEDA or PIPA.

Taking into consideration the steps already taken by TJX, the Commissioners recommended that TJX (i) provide them with a summary of its audit, including findings and recommendations; (ii) notify them of how it will monitor its systems more vigorously; and (iii) complete the conversion to higher encryption standards, itemize these standards, and notify them of the conversion's completion.

Outcome: TJX complied with the Commissioners' recommendations in such a manner that they deemed the safeguard component of the complaint to be "well-founded and resolved" by the Office of the Privacy Commissioner of Canada and "resolved" by the Alberta Office of the Information and Privacy Commissioner.

Fine Imposed: None

General Security Requirements Under U.S. Laws

Several US states have enacted security requirements, to generally require unregulated companies to implement security controls. In 2004, California became the first state to require companies to generally secure sensitive personal information.[86] This law imposed security requirements on companies that were not subject to the Gramm-Leach-Bliley Act, HIPAA or another security law. Since then, other states have followed suit, requiring (in some cases) specific security controls such as specific

security policies[87] or encryption.[88] Violations of these laws are generally actionable by state attorneys general. In some cases, a private right of action exists as well.

THE LIFETIME FITNESS CASE (AUGUST 2007)[89]

Respondent: Lifetime Fitness, Inc. and affiliates (collectively, "Lifetime")

Regulators: Texas State Attorney General

Basis for Complaint: Violations of (i) Chapter 48 of the Texas Business and Commerce Code known as the Texas Identity Theft Enforcement and Protection Act, (ii) Chapter 35 of the Texas Business and Commerce Code, (iii) the Texas Deceptive Trade Practices-Consumer Protection Act, and (iv) the Texas Health Spa Act.

Facts and Allegations: The complaint alleged that Lifetime collected large amounts of sensitive personal information, which they promise to safeguard in their online privacy statements and which they are obligated to safeguard under Texas law. The complaint further alleged that Lifetime did not safeguard the personal information; they permitted more than 100 business records containing sensitive information (such as Social Security numbers, driver's license numbers and credit card numbers) to be dumped in publicly-accessible trash dumpsters adjacent to the fitness center facilities.

The Complaint notes that:

- The information security provisions of the Texas Business and Commerce Code require companies to properly dispose of business records containing personal information, and, more specifically, dispose of such records by shredding or erasing or other means, so as to make the personal identifying information unreadable or undecipherable;

- The Texas Identity Theft Prevention Law requires companies to (1) implement and maintain reasonable procedures to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained in the regular course of business; and (2) destroy or arrange for the destruction of customer records containing sensitive personal information by shredding, erasing, or otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means; and

- The Texas Deceptive Trade Practices Act prohibits companies from (1) representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, when they are of another; and (2) failing to disclose information concerning goods or services which was known at the time of the transaction, if such failure would induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

Outcome: The Complaints asked the court to impose temporary and permanent injunctions on Lifetime, enjoining them from violating the laws by:

(1) Using false, misleading or deceptive statements to describe their privacy and security practices;

(2) Disposing of records containing sensitive personal information without first shredding or otherwise making the sensitive personal information unreadable; or

(3) Failing to protect and safeguard personal information from unlawful use or disclosure and exposing the data to risk of identity theft.

The complaint further asks the court to order Lifetime to adopt, implement and maintain a comprehensive information security program that is fully documented and in writing, and which includes reasonable procedures to protect and safeguard from unlawful use, disposal, or disclosure of any personal identifying or sensitive personal information collected or maintained by Lifetime in the regular course of business.

The complaint asks the court to impose civil penalties on Lifetime consisting o f $500 for each business record that it failed to properly dispose of in accordance with section 35.48 of Texas Business and Commerce Code, up to $50,000 for each violation of the Identity Theft Enforcement and Protection Act; and up to $20,000 per violation of the Deceptive Trade Practices Act.

The complaint also asks the court to order Lifetime to compensate any individuals for any losses, to provide for prejudgment interest on all awards or restitution, damages, and civil penalties as provided by the laws and to award reasonable attorney fees and costs as provided by the laws.

Fine Imposed: [unknown - compliant has not yet been resolved]

On January 10, 2008, the Texas attorney general issued a press release announcing the filing of a complaint against Select Physical Therapy Texas Limited Partnership, and its parent, Select Medical Corporation, a national health services provider, for failure to protect sensitive consumer records.[90] As in the Lifetime Fitness case, the attorney general charged the companies with violating the state's 2005 Identify Theft Enforcement and Protection Act as well as the secure disposal requirements in Chapter 35 of the Texas Business and Commerce Code. The complaint seeks significant damages. The press release noted that this action follows similar proceedings brought by the attorney general against CVS Pharmacy, Radio Shack, CNG Financial Corporation (which operates Check 'n Go stores), EZPAWN and EZMONEY Loan Services.

Even in the absence of a specific law requiring information security, the Federal Trade Commission has concluded that the failure to have reasonable security for sensitive information is an unfair trade practice.

THE DSW CASE (MARCH 2006)[91]

Respondent: DSW, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Unfair Trade Practices, Violation of Section 5 of the FTC Act

Facts and Allegations: Respondent is an Ohio based footwear company with locations in 32 states. DSW used wireless computer networks to request and obtain authorization for purchases made with credit cards, debit cards and checks. In order to obtain approvals for these purchases, personal information was collected from either the magnetic strip on the payment card or via magnetic ink character recognition from checks. An authorization request containing this personal information was transmitted via wireless computer networks from the cash register to a computer network located in the store and then on to the appropriate bank or check processor. DSW stored the collected personal information on in-store and corporate computer networks.

The FTC complaint alleged that DSW failed to employ reasonable and appropriate security measures to protect the personal information stored on its computer network, and that this failure caused or is likely to cause substantial injury to consumers. The FTC classified this conduct as unfair under section 5(a) of the FTC Act.

In particular, DSW allegedly failed to provide reasonable and appropriate security for the personal information collected at its stores by:

- Storing personal information in multiple files when it no longer had a business need to keep it;
- Not using readily available security measures to limit access to its computer networks through wireless access points on the networks;
- Storing the information in unencrypted files that could be easily accessed using a commonly known user ID and password;
- Not sufficiently limiting the ability of computers on one in-store network connecting with computers on another in-store or corporate network; and
- Not employing sufficient measures to detect unauthorized access.

These vulnerabilities allowed a hacker to obtain unauthorized access to the personal data of approximately 1.5 million consumers by using the wireless access points on one in-store computer network to access personal information on other in-store and corporate networks.

Outcome: The FTC entered into a consent decree with DSW, ordering:

Security Program: DSW shall establish, implement and maintain a well-documented, comprehensive information security program reasonably (1) designed to protect the security, confidentiality, and integrity of consumers' personal information and (2) contain administrative, technical and physical safeguards appropriate for the size, complexity, nature, and scope of its business.

Requirements of Security Program: The program shall include:

(1) Designation of an employee responsible for the security program;

(2) Identification of internal and external threats to security, confidentiality, and integrity of personal information through an assessment focusing on employee training, information systems, and potential system failures;

(3) Design and implementation of reasonable safeguards to identified risks; and

(4) Evaluation and adjustment of the information security program according to assessment and any material changes in business.

Third Party Audit: Within 180 days after service of order and thereafter biannually for twenty years, DSW must obtain an assessment and report from an independent, third party that:

(1) Sets forth the specific safeguards implemented and maintained by DSW;

(2) Explains how such safeguards are appropriate for the size and complexity of DSW, the nature and scope of DSW's activities and the sensitivity of the consumers' information;

(3) Explains how the implemented safeguards meet or exceed the protections required above; and

(4) Certifies that DSW's security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

Maintenance of Relevant Documents: DSW shall maintain and provide upon request:

(1) For a period of five years, a copy of any document that contradicts, qualifies, or calls into question DSW's compliance with the order; and

(2) For a period of three years after each biennial assessment retain a copy of all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments.

Delivery of Order: For a period of ten years, DSW shall deliver a copy of the FTC order to all current and future principals, officers, directors, and managers and to all current and future employees, agents and representatives with managerial responsibility over the subject matter.

Reporting: DSW shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Within 180 days after service of order and thereafter as requested, DSW shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None