

Complaint

IN THE MATTER OF**DSW INC.****CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT**

*Docket C-4157; File No. 0523096
Complaint, March 7, 2006--Decision, March 7, 2006*

This consent order relates to personal information collected from consumers by respondent DSW, Inc., which sells footwear for men and women at approximately 190 stores in 32 states. DSW stored consumers' personal information on computer networks and failed to employ reasonable and appropriate security measures to protect the information, leading to some fraudulent charges on accounts that consumers had used at DSW's stores. The order requires DSW to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers. The order also requires DSW to obtain periodic assessments and reports from a qualified, objective, independent third-party professional, certifying, among other things, that DSW has in place a security program that provides protections that meet or exceed the protections required by this order, and DSW's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information have been protected. Additional provisions relate to reporting and compliance.

Participants

For the Commission: *Molly Crawford, Laura Kaufmann, Laura Mazzearella, Jessica Rich, and Joel Winston.*

For the Respondent: *William C. MacLeod, Collier Shannon Scott PLLC; and Benita Kahn and James E. Phillips, Vorys, Sater, Seymour & Pease LLP.*

COMPLAINT

The Federal Trade Commission, having reason to believe that DSW Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

Complaint

1. Respondent DSW Inc. is an Ohio corporation with its principal office or place of business at 4150 East 5th Avenue, Columbus, Ohio 43219.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.
3. Respondent sells footwear for men and women at approximately 190 stores in 32 states. Consumers pay for their purchases with cash, credit cards, debit cards, and personal checks.
4. For credit card, debit card, and check purchases at its stores, respondent uses computer networks to request and obtain authorization for the purchase. To obtain card authorization, respondent collects information from consumers, including name, card number and expiration date, and certain other information. To obtain approval for payments by check, respondent collects the routing number, account number, check number, and the consumer’s driver’s license number and state (collectively, “personal information”).
5. For a credit or debit card purchase, respondent typically collects the information from the magnetic stripe of the credit or debit card. The information collected from the magnetic stripe includes, among other things, a security code used to verify electronically that the card is genuine. This code is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process. For purchases using a check, respondent typically collects information from the check using Magnetic Ink Character Recognition (“MICR”) technology. In each case, respondent collects the information at the cash register and wirelessly transmits the information, formatted as an authorization request, to a computer network

Complaint

located in the store (“in-store computer network”). The authorization request is then transmitted to the appropriate bank or check processor, which sends a response back to respondent through the same networks. Until at least March 2005, respondent stored personal information used to obtain credit card, debit card, and check authorizations, including magnetic stripe data, on in-store and corporate computer networks.

6. Respondent operates wireless access points through which the cash registers connect to the in-store computer networks. Other wireless access points are used to transmit information about respondent’s inventory from in-store scanners to the in-store computer networks.
7. Until at least March 2005, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information collected at its stores. Among other things, respondent (1) created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information; (2) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and (5) failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks.
8. In March 2005, respondent issued a press release stating that credit card and other purchase information stored on its computer networks had been stolen. In April 2005, respondent issued another press release listing the locations

Complaint

of 108 stores that were affected by the breach, and stating that checking account and driver's license numbers also had been subject to the breach. In April 2005, respondent also began sending notification letters to customers for whom it had or obtained addresses.

9. The breach compromised a total of approximately 1,438,281 credit and debit cards (but not the personal identification numbers associated with the debit cards), along with 96,385 checking accounts and driver's license numbers. To date, there have been fraudulent charges on some of these accounts. Further, some customers whose checking account information was compromised were advised to close their accounts, thereby losing access to those accounts, and have incurred out-of-pocket expenses such as the cost of ordering new checks. Some of these checking account customers have contacted DSW requesting reimbursement for their out-of-pocket expenses, and DSW has provided some amount of reimbursement to these customers.
10. As described in Paragraph 7 above, respondent's failure to employ reasonable and appropriate security measures to protect personal information and files 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 and is an unfair act or practice.
11. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

THEREFORE, the Federal Trade Commission this seventh day of March, 2006, has issued this complaint against respondent.

By the Commission.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*; and

Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Respondent DSW Inc. is an Ohio corporation with its principal office or place of business at 4150 East 5th Avenue, Columbus, Ohio 43219.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and check number; (h) a driver’s license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above.
2. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. Unless otherwise specified, “respondent” shall mean DSW Inc., its successors and assigns and its officers, agents, representatives, and employees.

Decision and Order

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other system failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment,

Decision and Order

and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

- D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic personal information collected from or about consumers;

Decision and Order

- C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP); a person qualified as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each

Decision and Order

document relating to compliance with the terms and provision of this order, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the reporting period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that, for a period of ten (10) years after the date of service of this order, respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities with respect to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after the date of service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary,

Decision and Order

parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address; *provided, however*, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred eighty (180) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Paragraph in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Decision and Order

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

**Analysis of Proposed Consent Order
to Aid Public Comment**

The Federal Trade Commission has accepted a consent agreement, subject to final approval, from DSW Inc. (“DSW”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received and will decide whether it should withdraw from the agreement and take other appropriate action or make final the agreement’s proposed order.

As described in the Commission’s proposed complaint, DSW sells footwear for men and women at approximately 190 stores in 32 states. Consumers pay for their purchases with cash, credit cards, debit cards, and personal checks. In the course of seeking approval for credit and debit card purchases, DSW collects consumers’ personal information, including name, card number and expiration date, and other information, from magnetic stripes on the cards. The information collected from the magnetic stripe is particularly sensitive because it contains a security code which can be used to create counterfeit cards that appear genuine in the authorization process. In the course of seeking approval for personal check purchases, DSW also collects consumers’ personal information, including routing number, account number, check number, and the consumer’s driver’s license number and state, from the check using Magnetic Ink Character Recognition (“MICR”) technology.

The Commission’s proposed complaint alleges that DSW stored consumers’ personal information on computers on networks located at both the store and corporate levels and failed to employ reasonable and appropriate security measures to protect the information. The complaint alleges that this failure was an unfair practice because it caused or was likely to cause substantial consumer injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition.

Analysis to Aid Public Comment

In particular, the complaint alleges that until at least March 2005, DSW engaged in a number of practices which, taken together, failed to provide reasonable security for sensitive personal information, including: (1) creating unnecessary risks to personal information collected at its stores by storing it in multiple files when it no longer had a business need to keep the information; (2) failing to use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) storing the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) failing to sufficiently limit the ability of computers on one in-store computer network to connect to computers on other in-store and corporate networks; and (5) failing to employ sufficient measures to detect unauthorized access. The complaint further alleges that there have been fraudulent charges on accounts that consumers had used at DSW's stores. Additionally, some consumers whose checking account information was compromised were advised to close their accounts, thereby losing access to those accounts, and incurred out-of-pocket expenses such as the cost of ordering new checks.

The proposed order applies to personal information from or about consumers that DSW collects in connection with its business. It contains provisions designed to prevent DSW from engaging in the future in practices similar to those alleged in the complaint.

Specifically, Part I of the proposed order requires DSW to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to DSW's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected. Specifically, the order requires DSW to:

- Designate an employee or employees to coordinate and be accountable for the information security program.

Analysis to Aid Public Comment

- Identify material internal and external risks to the security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operation or business arrangements, or any other circumstances that DSW knows or has reason to know may have a material impact on the effectiveness of its information security program.

Part II of the proposed order requires that DSW obtain within 180 days, and on a biennial basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) DSW has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order, and (2) DSW's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected. This provision is substantially similar to comparable provisions obtained in prior Commission orders under Section 5 of the FTC Act. *See, e.g., BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

Parts III through VII of the proposed order are reporting and compliance provisions. Part III requires DSW to retain documents relating to compliance. For the assessments and supporting documents, DSW must retain the documents for three (3) years after

Analysis to Aid Public Comment

the date that each assessment is prepared. Part IV requires dissemination of the order now and for the next ten (10) years to persons with supervisory responsibilities. Part V ensures notification to the FTC of changes in corporate status. Part VI mandates that DSW submit compliance reports to the FTC. Part VII is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.

Complaint

IN THE MATTER OF
HEALTH CARE ALLIANCE OF LAREDO, L.C.

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket C-4158; File No. 0410097
Complaint, March 23, 2006--Decision, March 23, 2006

This consent order addresses actions of Health Care Alliance of Laredo, L.C., in orchestrating and implementing agreements among its physician members to fix prices and other terms on which they would deal with health plans, and to refuse to deal with such purchasers except on collectively determined terms. Health Care Alliance forced numerous health plans to raise the fees paid to its physician members, and thereby raised the cost of medical care in the Laredo, Texas, area. The order requires the respondent to cease and desist from entering into or facilitating any agreement between or among any physicians (1) to negotiate on behalf of any physician with any payor; (2) to deal, refuse to deal, or threaten to refuse to deal with any payor; (3) regarding any term, condition, or requirement upon which any physician deals, or is willing to deal, with any payor, or (4) not to deal individually with any payor, or not to deal with any payor through any arrangement other than Health Care Alliance. The order requires the respondent, for three years, to notify the Commission before entering into any arrangement to act as a messenger, or as an agent on behalf of any physicians, with payors regarding contracts. The respondent is not precluded from engaging in conduct that is reasonably necessary to form or participate in legitimate joint contracting arrangements among competing physicians. The order also requires the respondent to distribute the complaint and order to all physicians who have participated in Health Care Alliance, and to payors that negotiated contracts with it or indicated an interest in doing so. In addition, the respondent is required, at any payor's request and without penalty, to terminate its current contracts with respect to providing physician services.

Participants

For the Commission: *John DeGeeter, Daniel P. Ducore, Tom Iosso, David R. Pender, Connie Salemi, Anne Schenof, and Louis Silvia.*

For the Respondent: *Gary Hall, Esq.*