THE PRIVACY CASE BOOK:

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

CHAPTER 3
Unfair Trade Practices

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

Chapter Three
UNFAIR TRADE PRACTICES

An **unfair trade practice** is any commercial conduct that causes substantial injury that is not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition.[67]

Many regulators are authorized to bring enforcement actions to address unfair trade practices. For example, under Section 5 of the FTC Act, the Federal Trade Commission can address conduct that is unfair, even if the conduct does not include any deception, misrepresentation or fraud. However, unlike the authority to address deceptive trade practices (which virtually all regulators share), some consumer protection laws do not prohibit conduct that is merely unfair. In these jurisdictions, regulators either have to allege deception or find another legal theory to support a regulator action.

Privacy Policy Changes

The Gateway Learning case represents the first action brought by the Federal Trade Commission using the unfairness doctrine to address a privacy violation. The Federal Trade Commission found that Gateway Learning's retroactive application of a materially-changed privacy policy to information it had previously collected from consumers was an unfair practice. Howard Beales, Director of the Federal Trade Commission's Bureau of Consumer Protection said: "It's simple – if you collect information and promise not to share, you can't share unless the consumer agrees. You can change the rules but not after the game has been played."[68]

THE GATEWAY LEARNING CASE (SEPTEMBER 2004)[69]

Respondent: Gateway Learning, Inc.

Regulator: Federal Trade Commission

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

Facts and Allegations: Respondent markets educational aids for children such as the popular, "Hooked on Phonics" audio spelling program. The company's primary customers include parents and teachers. The company had a posted privacy notice on its website that said it would not share personal information with third parties without the consumer's consent. The privacy notice also included a notice that the statement could be changed at any time.

In April 2003, Gateway Learning began renting personal information provided by consumers that the company had captured through online mechanisms on its website. Such information included first and last name, address, phone number, and purchase history. Gateway Learning did not seek or receive any consent from the consumers.

Further, the company released personal information (such as the age range and gender of consumers' children) to third parties for the purposes of direct mail and telemarketing solicitations on behalf of Gateway Learning.

To justify its sharing of the customer information, Gateway Learning posted a revised privacy notice on its website on June 20, 2003 notifying consumers that their personal information would be shared and providing them with a post office address where they could send a letter if they wanted to opt-out of such sharing. Gateway Learning posted a second revised privacy policy on July 17, 2003, but took no additional steps to notify consumers of the information change in the policy.

The FTC alleged that:

- Despite initial promises to the contrary, Gateway Learning rented personal information collected from consumers to third parties without receiving consumers' explicit consent and did provide personal information about children under the age of 13 without providing notice to consumers of material changes to its information practices;

- Gateway Learning retroactively applied its materially changed and revised privacy policy to information collected under the original privacy statement; and

- Substantial injury to consumers occurred.

The FTC also characterized the retroactive application of a materially-changed privacy policy to previously collected information as unfair and the failure to provide notice to consumers of material changes to the privacy policy as promised as misleading.

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

Bar on Misrepresentation: Gateway Learning shall not misrepresent (i) that they will not sell, rent, or loan to third parties such personal information; (ii) that they will not provide to any third party personal information about children under the age of thirteen; (iii) the manner Gateway Learning notifies customers of changes to its privacy policy; or (iv) the manner Gateway Learning will collect, use, or disclose personal information.

Ban on Disclosure of Personal Information to 3rd Parties:

(1) Gateway Learning shall not disclose to any third party any personal information collected on the website prior to the date it posted its revised privacy policy permitting third-party sharing (June 20, 2003), without first obtaining the express, affirmative (opt-in) consent of the consumer to whom such personal information relates.

(2) Gateway Learning shall not apply material privacy policy changes to information collected from or about consumers before the date of the posting, unless it obtained the express, affirmative (opt-in) consent of the consumers to whom such personal information relates.

Maintenance of Relevant Documents: For a period of five years, Gateway Learning must make available to the FTC all documents demonstrating compliance with the order, including:

(1) A copy of each different privacy statement or communication with the date, full text, html address, and graphics;

(2) A copy of documents seeking to obtain opt-in consent of consumers and any documents demonstrating such consent provided by consumers; and

(3) All invoices, communications, and records relating to the disclosure of personally identifiable information to third parties.

Delivery of Order: Gateway Learning must deliver a copy of this order to all current and future principals, officers, directors, managers and all employees with managerial responsibility over the subject matter of the order.

Reporting: Gateway Learning shall notify the FTC at least 30 days prior to any corporate change which may affect its compliance with the order. Within 60 days after service of order and thereafter as requested, Gateway Learning shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: $4,608 (which reflected all profits received for renting personal information)

Misuse of Customer Data

In the CartManager case, the Federal Trade Commission addressed a service provider using its customers' data for its own purposes.

THE CARTMANAGER CASE (MARCH 2005)[70]

Respondent: Vision I Properties, LLC doing business as CartManager International.

Regulator: Federal Trade Commission

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

Facts and Allegations: Vision I Properties licenses its CartManager shopping cart software and related e-commerce technologies and services to small and medium sized online merchants. These include "check out" services and shopping pages that are designed to look like the merchants' own websites. These pages collect personal information such as name, billing and shipping addresses, phone number, email address and credit card numbers as well as the contents of each online purchase made by consumers.

Because the CartManager web pages looked like the merchant's web pages, website customers assumed that the merchants' privacy policies applied to the personal information collected at checkout. CartManager did not disclose that the checkout pages were actually a separate website with its own data sharing policy or that it would use the consumers' information outside of the scope of the merchants' posted privacy policies.

The FTC complaint alleged that:

- CartManager did not adequately inform merchants or consumers that its information collection and use policies were inconsistent with the merchants' privacy policies or that it would disseminate the customer information to third parties.

- In January 2003, CartManager rented consumers' personal information collected through shopping cart and checkout pages generated by its software at its merchants' websites to third parties for marketing purposes.

The FTC classified CartManager's acts and practices as unfair and deceptive under Section 5 of the FTC Act. It also maintained that substantial consumer injury occurred and was not offset by countervailing benefits to consumers or competition and not reasonably avoidable.

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

Bar on Misrepresentation: CartManager shall not make any false or misleading representation regarding the collection, use, or disclosure of personally identifiable information.

Ban on Disclosure of Personal Information to 3rd Parties:

(1) CartManager shall not sell, rent, or disclose to any third party for marketing purposes any personally identifiable information that was collected from consumers through shopping cart software using a merchant customer's website prior to the date of this agreement.

(2) CartManager shall not sell, rent, or disclose to any third party for marketing purposes any personally identifiable information that was collected from consumers through shopping cart software using a merchant customer's website after the date of this agreement unless:

(a) The company provides to each merchant a clear and conspicuous written notice of information practices and obtains the merchant's certification it will (i) post a privacy policy informing customers of such policies or (ii) notify customers that they are leaving merchant's website when enter shopping cart and checkout pages; or

(b) The company provides a clear and conspicuous disclosure on pages collecting information that consumers are on CartManager pages and that collected personal information will be used, sold, rented, or disclosed to third parties for marketing purposes.

Maintenance of Relevant Documents: None.

Delivery of Order: CartManager shall deliver to each current or future principals, officers, directors, managers and to all employees with managerial responsibility over the subject matter a copy of the FTC order.

Reporting: CartManager shall notify the FTC at least 30 days prior of any corporate change which may affect its compliance with the order. Within 60 days after service of order and thereafter as requested, CartManager shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None

In analyzing the CartManager order, it is important to note that the merchants were generally *not* aware of CartManager's use and disclosure of the consumer data for its own purposes. As part of the finding of unfairness, the Federal Trade Commission determined that CartManager had not adequately informed its merchants customers (or the ultimate consumers) that its information collection and use policies were inconsistent with the merchants' privacy policies. Had the merchants been aware that their service provider was using personal information contrary to their published privacy notices, the merchants could have faced liability under Section 5 of the FTC Act as well.

Inadequate Security

As discussed more fully in Chapter 4, the Federal Trade Commission has also concluded that it is an unfair trade practice to collect sensitive personal information (such as credit card numbers) unless

reasonable security exists to protect the information. According to Federal Trade Commission Chairman Deborah Platt Majoras,

> *Consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security. This case [against BJ's Wholesale Club] demonstrates our intention to challenge companies that fail to protect adequately consumers' sensitive information.*[71]

THE BJ'S WHOLESALE CLUB CASE (SEPTEMBER 2005)[72]

Respondent: BJ's Wholesale Club Inc.

Regulator: Federal Trade Commission

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

Facts and Allegations: BJ's is a discount retailer based in Natick, Massachusetts that has approximately 150 stores and 78 gas stations located in 16 states. BJ's sells brand-name food and general merchandise items to consumers who have purchased "memberships" that allow them to shop in the stores. At the time of the complaint, BJ's had approximately 8 million members.

When consumers made purchases in the BJ's Club stores using payment cards, BJ's used an in-store computer networks to request and obtain authorization from the card-issuing banks. In order to obtain approvals for these purchases, personal information was collected from the magnetic strip on the consumer's card. An authorization request containing this personal information was transmitted from the in-store computer network to the company's central datacenter and then on to the issuing bank. The bank's response was received through the same computer network. BJ's stored this collected personal information on in-store and corporate computer networks. BJ's also operated wireless access points on its in-store computer networks to manage inventory with wireless inventory scanners.

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

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

- Failing to encrypt personal information both while in transit and when stored on in-store computer networks;
- Storing the information in files that could be easily accessed using a commonly known default user ID and password;
- Failing to use readily available security measures to limit access to its computer networks through wireless access points on the networks;
- Not employing sufficient measures to detect unauthorized access or conduct security investigations; and

- Creating unnecessary risks to the personal information by storing it for up to 30 days, even when it no longer needed the information.

These vulnerabilities allowed a hacker to obtain unauthorized access to the personal data of BJ's customers by using the wireless access points on an in-store computer network to access personal information on the network. Several million dollars in fraudulent purchases were then made using counterfeit copies of credit and debit cards containing personal information that was stored on BJ's computer network.

Outcome: The FTC entered into a consent decree with BJ's, ordering:

Security Program: BJ's shall establish, implement and maintain a well-documented, comprehensive information security program reasonably designed to (1) 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, BJ's must obtain an assessment and report from an independent, third party that:

(1) Sets forth the specific safeguards implemented and maintained by BJ's;

(2) Explains how such safeguards are appropriate for the size and complexity of BJ's, the nature and scope of BJ'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 BJ's security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

Maintenance of Relevant Documents: BJ's 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 BJ'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: BJ's 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: BJ's 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, BJ's shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None