Introduction

The following guide describes key U.S. Federal Trade Commission (FTC) and U.S. state attorneys general enforcement actions that have been brought in the privacy and security areas over the past several years. It is excerpted from “The IAPP Information Privacy Case Book: A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risk” by Margaret P. Eisenhauer, Esq., CIPP (IAPP, 2008). ISBN #978-0-9795901-2-2.

The guide is intended for informational purposes only and does not represent legal advice. Whether or not you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Studying the various cases described in this guide can provide insights into the types of enforcement priorities that the FTC and U.S. state attorneys general have established as well as the steps that the Commission feels are important for proper consumer protection in the privacy and security arenas. Copies of the actual FTC cases—as well as information on additional FTC privacy and security actions— are available online from the FTC Web site: http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

Who Should Review

**CIPP Certification Candidates:** These case summaries present a number of privacy and security concepts and issues that are addressed under the Certified Information Privacy Professional (CIPP) credentialing program. You are strongly encouraged to understand these cases as a supplement to your formal exam preparation, such as the CIPP Training Workshop and The IAPP Certification Training Series on CD-ROM.

**Other Privacy Professionals:** This guide may serve as a useful reference in understanding the basic components of privacy and security enforcement actions taken to date in the United States.

Acknowledgements

The IAPP extends its sincere thanks to the author, Peggy Eisenhauer, CIPP, Founder of Privacy & Information Management Services – Margaret P. Eisenhauer, P.C. (“PIMS”) and CIPP Certification Advisor, as well as Tanya Wilson, PIMS Practice Administrator.
Contents

I. GENERAL THEORIES OF LIABILITY ......................................................... 5
   Regulators .......................................................................................... 5
   Privacy Enforcement Powers ............................................................... 5
   The Authority of the U.S. Federal Trade Commission .......................... 8
   Regulatory Processes .......................................................................... 8
   Analysis of an FTC Consent Decree .................................................. 10

II. DECEPTIVE TRADE PRACTICES ......................................................... 17
   Privacy and Security Promises ............................................................ 17
   The Microsoft Case – Federal Trade Commission (U.S.) ....................... 17
   The Eli Lilly Case – Federal Trade Commission (U.S.) ......................... 19
   The Eli Lilly Case – State Attorneys General (U.S.) ............................... 20
   The PetCo Case – Federal Trade Commission (U.S.) ............................. 22
   Pretexting .......................................................................................... 23
   The HP Civil Case – California State Attorney General (U.S.) ................. 23

III. UNFAIR TRADE PRACTICES ............................................................ 25
    Privacy Policy Changes .................................................................... 25
    Misuse of Customer Data .................................................................. 27
    The CartManager Case – Federal Trade Commission (U.S.) ................. 27
    Inadequate Security .......................................................................... 29
    The B.J.’s Wholesale Club Case – Federal Trade Commission (U.S.) ....... 29

IV. INFORMATION SECURITY ................................................................. 31
    Security Requirements for Regulated Entities .................................... 31
    The Superior Mortgage Case – Federal Trade Commission (U.S.) .......... 31
    General Security Requirements Under U.S. Laws ............................. 33
    The Lifetime Fitness Case – Texas State Attorney General (U.S.) ............ 33
    The DSW Case – Federal Trade Commission (U.S.) ........................... 35
V. MARKETING COMMUNICATIONS ................................................................. 36

Telemarketing .......................................................................................... 37
  The DirecTV, Inc Case – Federal Trade Commission (U.S.) ...................... 38
  The Broadcast Team Case – Federal Trade Commission (U.S.) ............... 40
  The Craftmatic Case – Federal Trade Commission (U.S.) ......................... 41
  The MarketLinkx Case – Missouri State Attorney General (U.S.) ............ 42

Fax Communications .................................................................................. 43
  The Fax.com Case – Federal Trade Commission (U.S.) ......................... 43

E-mail Communications ............................................................................. 44
  The Member Source Media Case – Federal Trade Commission (U.S.) ....... 44

VI. E-COMMERCE AND ONLINE ACTIVITIES ............................................. 46

User-installed Software ............................................................................ 46
  The Sony/BMG Cases – Federal Trade Commission (U.S.) .................... 46
  The DirectRevenue Case – Federal Trade Commission (U.S.) ............... 50
  The Internet Advertisers Case – New York State Attorney General (U.S.) 53

Social Networking Web sites ..................................................................... 54
  The Facebook Case – New York State Attorney General (U.S.) .............. 54
  The MySpace Case – State Attorneys General (U.S.) ......................... 55

VII. SPECIFIC U.S. PRIVACY LAWS AND REGULATED DATA TYPES ....... 56

Personal Information of Children .............................................................. 57
  The Hershey Case – Federal Trade Commission (U.S.) ....................... 57
  The Xanga Case – Federal Trade Commission (U.S.) ......................... 58
  The Santa.com Case – Texas State Attorney General (U.S.) .................. 60

Consumer Reporting Data and Credit Information .................................. 61
  The ChoicePoint Case – Federal Trade Commission (U.S.) ............... 61
  The Quicken Loans Case – Federal Trade Commission (U.S.) ............. 64
  The American United Mortgage Case – Federal Trade Commission (U.S.) 65

Healthcare Information and Medical Records ........................................ 65
  The HIPAA Privacy Rules Case – Office of Civil Rights (U.S.) ............ 66
I. General Theories of Liability

Companies face two main types of legal claims from regulators as a result of their information handling practices: (1) claims that the company has violated a specific law or regulation, and (2) claims that the company has violated a general consumer protection law, such as a legal obligation to conduct business in a fair and non-deceptive manner. Regulators bring such claims as a result of privacy or security incidents, consumer complaints or independent regulatory inquiry.

Regulators

A regulator is any government agency with the ability to investigate a company’s information handling practices or bring an action against a company for privacy or security violations.

In countries with national data protection laws, regulators include the data protection authorities, agencies established by these laws to oversee and implement the laws as well as those government agencies that enforce consumer protection and labor laws. In the United States, the Federal Trade Commission ("FTC") and state attorneys general aggressively enforce privacy laws and consumer protection laws. Other regulators also include functional regulators, those government agencies that oversee companies engaged in specific businesses or activities, such as financial services, insurance, education, healthcare, or telecommunications.

Regulates the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce, excepting banks, savings and loan institutions, Federal credit unions and common carriers  
Receives complaints, conducts investigations and brings civil actions to protect consumers against unfair or deceptive trade practices; enforces Federal consumer protection laws and FTC rules; investigates company and industry practices  
Criminal actions referred to the US Department of Justice for prosecution |
| United States – Federal | Federal Communications Commission (FCC) – Enforcement Bureau  
Regulates interstate and international communications by radio, television, wire, satellite and cable in the 50 states, the District of Columbia and U.S. possessions  
Receives complaints, conducts investigations and brings actions to enforce the Communications Act and FCC rules |
<table>
<thead>
<tr>
<th>United States – Federal</th>
<th>Department of Health &amp; Human Services – Office of Civil Rights (OCR)</th>
<th>OCR investigates complaints of noncompliance with and makes decisions regarding the interpretation, implementation, and enforcement of the HIPAA Privacy Rule; authority delegated to the Director, OCR by the Secretary of the Department of HHS</th>
<th>Receives complaints, conducts investigations and brings actions to enforce the HIPAA Privacy Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States – Federal</td>
<td>Department of Health &amp; Human Services – Centers for Medicare and Medicaid Services (CMS)</td>
<td>CMS investigates complaints of noncompliance with and makes decisions regarding the interpretation, implementation, and enforcement of the HIPAA Security Rule; authority delegated to the Administrator, CMS by the Secretary of the Department of HHS</td>
<td>Receives complaints, conducts investigations and brings actions to enforce the HIPAA Security Rule</td>
</tr>
<tr>
<td>United States – Federal</td>
<td>Department of the Treasury – Office of the Comptroller of the Currency (OCC)</td>
<td>Charters, regulates and supervises all national banks, and supervises the federal branches and agencies of foreign banks</td>
<td>Brings supervisory actions against banks that do not comply with laws and regulations or that otherwise engage in unsound banking practices; OCC can remove officers and directors, negotiate agreements to change banking practices and issue cease and desist orders as well as civil money penalties</td>
</tr>
<tr>
<td>United States – States and Territories</td>
<td>Attorneys General (AG)</td>
<td>Varies due to constitutional and statutory mandates, but each AG serves as chief legal officer of its state, has jurisdiction over persons and entities within (or doing business within) its state, and represents the state and state agencies generally</td>
<td>Receives complaints, conducts investigations and brings actions to enforce Federal or State laws and addresses deceptive trade practices</td>
</tr>
</tbody>
</table>
The Authority of the U.S. Federal Trade Commission

In the United States, the Federal Trade Commission (“FTC”) is the Federal government agency primarily charged with consumer protection. In this role, it aggressively protects consumers, enforces company-made privacy and security promises and enforces obligations imposed on companies by specific privacy and security laws.

The basic consumer protection statute enforced by the Federal Trade Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful" (15 U.S.C. Sec. 45(a)(1)). Understanding the meanings of (and differences between) unfair and deceptive trade practices is crucial for interpreting Federal Trade Commission actions:

- **A deceptive trade practice** is commercial conduct that includes false or misleading claims, or claims that omit material facts. Consumer injury does not have to result, the mere fact that a company has engaged in a deceptive trade practice is actionable.

- **An unfair trade practice** is commercial conduct that (1) causes (or is likely to cause) substantial injury to consumers (2) that consumers cannot reasonably avoid themselves, and (3) without offsetting benefits to consumers or competition.

Accordingly, if a company makes a privacy or security promise, and then fails to live up to that promise, it has likely engaged in a deceptive trade practice. For example, if a company promises in a privacy notice not to share personal information, and then it shares the information, it has engaged in deceptive conduct.

If a company puts consumers at risks, with no offsetting benefit, this may be an unfair trade practice. For example, even if a company does not promise to have reasonable security for its website, if the company collects sensitive data (such as credit card numbers) without having reasonable security, the company has likely engaged in an unfair trade practice.

In addition, the Federal Trade Commission enforces a variety of specific consumer protection statutes, such as the Children's Online Privacy Protection Act ("COPPA"), the Fair Credit Reporting Act (FCRA), the privacy and safeguards regulations promulgated under the Gramm-Leach-Billey Financial Services Modernization Act of 1999 ("GLBA"), the Telemarketing Sales Rule ("TSR") and the CAN-SPAM Act. The authority to enforce specific laws (and to promulgate rules under these laws) is provided in the laws themselves. For example, COPPA, GLBA and the CAN-SPAM Act expressly give the Federal Trade Commission the power to make rules and to enforce the Acts and the rules.

It is important to note that the Federal Trade Commission’s authority is limited in some respects. For example, the FTC Act states that the Federal Trade Commission may not regulate or enforce against certain industries that are otherwise regulated, such as financial institutions subject to jurisdiction of the Office of Comptroller of the Currency, the Federal Reserve, et. al, and common carriers. The Federal agencies that regulate these industries often work closely with the Federal Trade Commission on privacy regulations, however. For example, the Federal Trade Commission works with a group of Federal financial institution regulators on GLBA rules, and it works with the Federal Communications Commission on telemarketing and email privacy rules as they relate to both financial institutions and common carriers.

Additionally, even where Federal Trade Commission authority does exist, companies are often subject to additional regulatory scrutiny. For example, companies often face both Federal Trade Commission and state attorney general actions for privacy or security breaches. Because the state attorneys general have independent authority, Federal Trade Commission actions do not preclude or supersede state action. In many cases, the consent decrees entered into with the state attorneys general for breaches exceed the Federal Trade Commission’s requirements. Fines are also common at the state level.
Regulatory Processes

As described above, regulators generally have broad powers to receive complaints, conduct investigations, resolve matters informally, and to bring formal enforcement actions. For example, if the Federal Trade Commission suspects that a company has not complied with applicable laws, it will typically launch an investigation of the company. Depending on the situation, the Federal Trade Commission may work with the company to resolve the matter informally. For more egregious breaches, or where the Federal Trade Commission detects a pattern of non-compliance, the Federal Trade Commission may bring a formal enforcement action against the company. These actions generally result in the Federal Trade Commission and the company entering into a settlement agreement or consent decree. The Federal Trade Commission has authority to include many different types of provisions in consent decrees, consistent with its role as a consumer protection agency.

Additionally, regulators often have broad discretion with regard to the terms they require to resolve investigations of companies. The case summaries illustrate the variety of provisions that regulators may demand. However, in the United States, there are also some common elements that are included in most settlement agreements. These common elements include:

1. A prohibition on misrepresentation of privacy or security program protections, and/or a prohibition on any further unfair, deceptive or non-compliant conduct;

2. A requirement to establish and maintain an appropriate compliance program or information security program; including, for security programs, (i) training and proper oversight of employees and agents, (ii) identification of reasonably foreseeable risks, (iii) the design of reasonable and appropriate controls and safeguards, and (iv) regular evaluation of the program;

3. An order to delete inappropriately collected information or disgorge inappropriately obtained revenue; and,

4. An obligation to maintain certain records and documents related to the company’s programs and compliance and to provide these records and documents upon request from the regulator; in some cases the company may be required to proactively notify the regulator of any change which may affect the company’s compliance.

In many cases, regulators will also require the company to pay a fine or provide money for restitution to the individuals who were harmed by the violation. Studying the various cases described in this guide can provide insight into the types of enforcement priorities that regulators have established as well as the steps that regulators believe are important for proper consumer protection in the privacy and security arena.
Analysis of an FTC Consent Decree

The following diagram presents a published Federal Trade Commission consent agreement, with annotations explaining the various parts and provisions. The particular agreement presented is the final order in the matter of the Federal Trade Commission vs. BJ's Wholesale Club.

**UNITED STATES OF AMERICA**
**FEDERAL TRADE COMMISSION**

**In the Matter of**
**BJ'S WHOLESALE CLUB, INC.**

**FILE NO. 452350**
**AGREEMENT CONTAINING CONSENT ORDER**

The Federal Trade Commission has concluded an investigation of certain acts and practices of BJ’s Wholesale Club, Inc., a Delaware corporation ("Respondent").

The Respondent has been represented by counsel, in writing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint.

Therefore,

IT IS HEREBY AGREED by and between BJ’S Wholesale Club, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. The Respondent is a Delaware corporation with its principal office or place of business at One Marcus Road, Marlborough, Massachusetts 01752.

2. The Respondent acknowledges all the jurisdictional facts set forth in the draft complaint.

3. The Respondent agrees:
   A. to pay the sum of $1.2 million, plus costs and expenses in the amount of $100,000;
   B. to pay $75,000 to the Federal Trade Commission as a civil penalty;
   C. to pay $20,000 to the Federal Trade Commission to cover filing fees;

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it is publicly released. The Commission does not

Identifies the "respondent" – in this case, the respondent is BJ’S Wholesale Club, Inc., a legal person (a corporation) under Delaware law.

The facts relate to a security incident involving credit card data.*

The respondent agrees to enter this order and waives various procedural rights. The respondent cannot later challenge the validity of the order or dispute the underlying facts. These provisions provide the FTC with a clear path for future action, if the respondent fails to meet the terms of this consent decree.
The respondent does not admit that it has violated any law. This statement is designed to limit the ability of other litigants to use this consent decree against the respondent.

Specific acknowledgement that the consent order may include a civil penalty (i.e., a fine).

Terms that are used in the order are defined to ensure that the respondent understands its obligations.

* The complaint is online at http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf.
In the complaint, the FTC alleged that:

"the 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 an unfair act or practice."

The steps ordered here are designed to provide the security necessary for fair trade practices. The respondent must implement specific controls and also have those controls assessed periodically by an independent third party. The respondent must provide copies of the initial assessment report to the FTC. Subsequent assessment reports are provided to the FTC upon request.

These provisions are common in FTC consent decrees involving claims of inappropriate security.
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 respondent shall:  

itself an assessment report; and

13

its assessment team, to be prepared by a person qualified as a Certified Information Systems Security Professional (CISP) or as a Certified Information Systems Auditor (CISA), a person holding Global Information Assurance Certification (GIAC) from Syxs.com, a senior analyst, 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 first assessment, as well as all plans, reports, studies, records, 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 is completed. All subsequent biennial Assessments shall be certified by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

Page 4 of 7
Consent decrees generally require the respondent to maintain compliance documents and provide them to the FTC upon request.

Consent decrees generally require the respondent to deliver copies of the order to individuals associated with the company (such as officers and employees) to ensure awareness of the obligations by everyone affected.

Consent decrees generally require the respondent to notify the FTC if any events occur that may affect the company’s compliance posture, such as a change of corporate ownership.

III

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a paper or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years, any documents, whether prepared by or on behalf of respondent, that constitute, clarify, 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 such biennial Assessment required under Paragraph II of this order, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and any materials, whether prepared by or on behalf of respondent, relating to respondent’s compliance with Paragraph I and II of this order for the compliance period covered by such biennial Assessment.

IV

IT IS FURTHER ORDERED that 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 managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such former 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, reorganization, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any act or practice subject to this order; the proposed filing of a bankruptcy petition; or a change in another corporate name or address. Provided, however, that, with respect to any proposed change in the corporation that which respondent becomes 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.
Consent decrees generally require the respondent to confirm in writing to the FTC that the company has complied with the order.

The term of this consent decree is generally 20 years, so long as another complaint is not filed alleging a violation of the order.

Under the FTC Act, violations of an FTC order are punishable by a civil penalty of up to $11,000 per violation.

The company and the FTC sign the consent decree, asserting their assent to the terms. When signed, this is a binding agreement.

The FTC will sign after a vote of the Commissioners.
FEDERAL TRADE COMMISSION

By

JULIA SIEGRIST
Counsel for the Federal Trade Commission

APPROVED:

JOEL WENSTON
Associate Director
Division of Financial Practice

LYDIA E. PARRISH
Director
Bureau of Consumer Protection
II. Deceptive Trade Practices

Virtually all regulators have the authority to address deceptive trade practices; companies that make false or misleading statements can be confident that their conduct is actionable universally. Many of the earliest privacy cases were brought to address deceptive trade practices, such as misrepresentations in company privacy notices.

Under Section 5(a) of the FTC Act, the Federal Trade Commission may address deceptive trade practices. Each state has a similar statute, enforceable by the state attorney general. As noted above, deceptive trade practices are commercial conduct that includes false or misleading claims, or claims that omit material facts. Consumer injury does not have to result, the mere fact that a company has engaged in a deceptive trade practice is actionable.

Privacy and Security Promises

THE MICROSOFT CASE (DECEMBER 2002)

Respondent: Microsoft Corporation

Regulator: Federal Trade Commission

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

Facts and Allegations: In 1998, Microsoft acquired a start-up software company called Firefly and its namesake online behavioral targeting technology. Microsoft subsequently renamed the technology “Passport” and deployed it across a number of partner and affiliate websites. The technology collected and stored personal information from consumers, which could be passed to other websites that had enabled the Passport technology.

Shortly after the product’s launch, a complaint was filed by a consumer group maintaining that Microsoft had misrepresented Passport’s underlying security measures as well as the information it collected. The FTC investigated Microsoft in response to this complaint.

The FTC complaint alleges that:

• Despite representations to the contrary by the company, Microsoft failed to implement and document procedures reasonable and appropriate to protect personal information because Microsoft did not use reasonable methods to (i) prevent and detect unauthorized access, (ii) monitor potential vulnerabilities, and (iii) record information to perform security audits.

• Microsoft collected certain information it claimed it did not, such as records of the sites to which a Passport user signed in, along with dates and times of sign in; and

• Purchases made through Passport were not safer and more secure than those made without Passport because the security procedure with or without Passport was identical.
**Outcome:** The FTC entered into a consent decree with Microsoft, ordering:

**Bar on Misrepresentation:** Microsoft shall not misrepresent its information practices, including:

1. The personal information collected;
2. Its efforts to maintain or protect the privacy, confidentiality or security of any personally identifiable information;
3. The steps it will take with respect to personal information it has collected in the event of a change in privacy policy; and
4. Parents’ ability to control the information their child can provide to participating sites or the use of such information.

**Security Program:** Microsoft shall establish and maintain a written security program that is (i) designed to protect the security, confidentiality and integrity of personal information, and (ii) appropriate for the size and complexity of Microsoft, the nature and scope of activities and the sensitivity of the information collected.

**Security Program:** Requirements of Security Program shall include:

1. Designation of a responsible employee(s);
2. Identification of risks to the security, confidentiality and integrity of consumer information that could result in unauthorized disclosure or misuse of information;
3. The designation and implementation of safeguards through risk assessment, testing and monitoring of the safeguards; and
4. Evaluation and adjustment of the security program as a result of the assessments, changes to Microsoft’s business or other circumstances which may have a material impact on the program.

**Third Party Audit:** Within one year and on a biannual basis thereafter, Microsoft must obtain an assessment and report from an independent third-party which certifies that the security program:

1. Meets or exceeds the protections set forth above; and
2. Is operating with sufficient effectiveness to provide reasonable assurance that consumer information has been protected.

**Maintenance of Relevant Documents:** For a period of five years Microsoft shall provide (upon request):

1. A copy of each representation made to consumers regarding the collection, use and security of collected information;
2. All plans, reports or other materials relating to Microsoft’s compliance with the order; and
3. Any document that contradicts, qualifies or questions Microsoft’s compliance with the order.
Delivery of Order: Microsoft shall deliver to each current or future director, employee, agent or representative a copy of the FTC order.

Reporting: Microsoft shall notify the FTC of any change which may affect its compliance with the order. Within 120 days after service of order and thereafter as requested, Microsoft shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: None

The Eli Lilly cases demonstrate how conduct can create enforcement risk for companies at both the Federal and the state levels.

THE ELI LILLY CASE (MAY 2002)

Respondent: Eli Lilly and Company

Regulator: Federal Trade Commission

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

Facts and Allegations: Respondent, a large U.S.-based pharmaceutical company, offered consumers an online reminder service called Medi-messenger. This service sent automated, personalized messages to registered consumers via electronic email that reminded them to take or refill their depression medications as individually prescribed.

Using a new software program, an Eli Lilly employee inadvertently sent an e-mail notice to all subscribers of the Medi-messenger service. This notice contained (for all to see) the e-mail addresses of all 669 individuals who were registered to the service at that time.

The FTC complaint alleged that Eli Lilly failed to implement or maintain reasonable and appropriate measures to protect consumer information including a failure to properly train employees, provide oversight, and implement appropriate checks and controls.

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

Bar on Misrepresentation: Eli Lilly shall not misrepresent the extent to which it maintains and protects the privacy or confidentiality of the collected personal information.

Security Program: Eli Lilly shall establish and maintain a security program for the protection of its collected personally identifiable information.

Requirements of Security Program: The program shall include:

(1) Designation of personnel to coordinate and oversee the program;

(2) Identification of risks to the security, confidentiality and integrity of personal information;
(3) An annual written review conducted by qualified persons to evaluate the effectiveness of the program and recommended changes; and

(4) Adjustments to the program based on the reviews, monitoring or any material changes in operations of Eli Lilly that affect the security program.

**Third Party Audit**: Not specified in the FTC order. However, Eli Lilly is required to have its annual internal written review examined and certified by an independent auditor. (Additionally, per the multi-state voluntary assurance agreement with certain state attorneys general (discussed below), Eli Lilly must undergo five annual, independent compliance reviews and report the findings of those reviews to the states.)

**Maintenance of Relevant Documents**: For a period of five years, Eli Lilly shall provide (upon request):

(1) A copy of each representation made to consumers regarding the collection, use and security of collected information;

(2) All plans, reports or other materials relating to, Eli Lilly’s compliance with the order; and

(3) Any document that contradicts, qualifies or questions, Eli Lilly’s compliance with the order.

**Delivery of Order**: Eli Lilly shall deliver to each current and future director, employee, agent or representative a copy of the FTC order.

**Reporting**: Eli Lilly shall notify the FTC of any change which may affect its compliance with the order. Within 120 days after service of order and thereafter as requested, Eli Lilly shall file a report with the FTC setting forth its compliance with the order.

**Fine Imposed**: None

---

**THE ELI LILLY CASE – STATE ATTORNEYS GENERAL (JUNE 2002)**

**Respondent**: Eli Lilly and Company

**Regulator**: Attorneys General of California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont (the “States”)


**Facts and Allegations**: The facts and allegations mirrored those in the FTC case regarding Medi-messenger discussed above.
**Outcome:** The States entered into an Assurance of Voluntary Compliance and Discontinuance Agreement with Eli Lilly, ordering:

**Bar on Misrepresentation:** Eli Lilly shall not misrepresent the extent to which it maintains and protects the privacy or confidentiality of collected personally identifiable information.

**Security Program:** Eli Lilly shall (a) establish supervisory procedures designed to achieve compliance with the Assurance, and (b) establish and maintain a security program for the protection of its collected personally identifiable information.

**Requirements of Security Program:** The program shall include:

1. Appropriate safeguards that are designed to protect personally identifiable information against unauthorized access, use or disclosure and against reasonably anticipated threats to its security or integrity;
2. Automated barriers that ensure only pre-authorized and designated personnel can gain access to the personally identifiable information;
3. Designation of personnel to coordinate and oversee the program;
4. Identification of risks to the security, confidentiality and integrity of personal information;
5. Training relevant employees to monitor compliance using materials and procedures that are current;
6. Documenting the means of implementing the program;
7. Within ninety days (and annually thereafter), a written review conducted by qualified persons to monitor compliance, evaluate the effectiveness and recommended changes to the program, in addition to monitoring the conformance of its practices to its representations; and
8. Adjustments to the program based on the reviews, monitoring or any material changes in the operations of Eli Lilly that affect the security program.

**Third Party Audit:** The annual audit may be performed by a qualified and independent third party. If the audit is performed internally then Eli Lilly is required to have its written review examined and certified by an independent third party that will report its results in writing to the States.

**Maintenance of Relevant Documents:** For a period of five years, Eli Lilly shall maintain and provide (upon request): a copy of each representation made to consumers regarding the collection, use and security of personally identifiable information; all plans, reports or other materials relating to Eli Lilly’s compliance with the order; and any document that contradicts, qualifies or questions, Eli Lilly’s compliance with the order.

**Delivery of Order:** Within thirty days of date of Assurance, Eli Lilly shall deliver a copy of the Assurance to all principals, officers, directors, managers, employees, agents, representatives and contractors having responsibility relating to the Assurance. The Assurance shall be delivered to future individuals and entities within thirty days of assuming their responsibilities.

**Fine Imposed:** $160,000
Early cases addressing security incidents were brought as deceptive trade practices cases, based on the companies’ security promises in their privacy notices. As a result of these actions, many companies revised their privacy notice language to avoid making promises about security. The regulators responded by interpreting the unfairness doctrine to encompass insufficient security.

**THE PETCO CASE (NOVEMBER 2004)**

**Respondent:** Petco, Inc.

**Regulator:** Federal Trade Commission

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

**Facts and Allegations:** Petco sells pet food, supplies, and services through its stores and on its website. Visitors communicate with the website using a web application to obtain product information and to supply transaction information such as credit card number and contact information. The Petco website has a posted privacy statement that promised appropriate privacy and security of the personal information provided to the company via the web application.

Since February 2001, the Petco website had been vulnerable to Structured Query Language (SQL) searches and other online exploits. In June 2003, a visitor conducted a SQL search and was able to read, in clear text, the credit card numbers stored within Petco’s database.

The FTC alleged that:

- Despite Petco’s representations to the contrary, personal information obtained from consumers was not maintained in an encrypted format and was thus accessible to persons other than the consumer providing the information; and

- Such information, including credit card numbers, was accessible through commonly known technical attack methods thereby failing to maintain reasonable and appropriate measures to protect personal information.

The FTC characterized Petco’s actions as deceptive, but did not allege consumer injury.

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

**Bar on Misrepresentation:** Petco shall not misrepresent the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of any personal information collected from or about consumers.

**Security Program:** Petco shall establish and maintain a comprehensive security program reasonably designed for the protection of its collected personally identifiable information. In creating the program, Petco shall:

1. Designate personnel to coordinate and oversee the program;
(2) Identify risks to the 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) Evaluate and adjust its program according to assessment and material changes in business.

Third Party Audit: Within 180 days after service of order and thereafter biannually for ten years, Petco must obtain an assessment and report from an independent, third party that (i) sets forth the specific safeguards implemented and maintained by Petco, (ii) explains how such safeguards are appropriate for the size and complexity of Petco, the nature and scope of Petco’s activities and the sensitivity of the information, (iii) explains how the safeguards meet or exceed the protections above; and (iv) certifies that Petco’s security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

Maintenance of Relevant Documents: For a period of five years, Petco shall provide (upon request):

(1) A copy of each representation made to consumers regarding the collection, use and security of collected information;

(2) All plans, reports or other materials relating to Petco’s compliance with the order; and

(3) Any document that contradicts, qualifies or questions Petco’s compliance with the order.

Delivery of Order: Petco must deliver a copy of this order to all current and future principals, officers, directors, managers and all employees with managerial responsibility.

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

Fine Imposed: None

Pretexting

Making false or misleading statements in a privacy notice is not the only deceptive conduct privacy regulators enforce. Regulators also bring action when personal information is collected via deceptive means.

“Pretexting” is defined as the practice of using false pretenses to gather personal information. Using pretexting to collect financial information is prohibited by the Gramm-Leach-Bliley Act, and the Federal Trade Commission has brought numerous enforcement actions to address this deceptive practice. State laws commonly prohibit the use of pretexting to obtain sensitive data, such as financial records or telephone records. The following summary presents a state attorney general action for pretexting.

THE HP CIVIL CASE (DECEMBER 2006)

Respondent: Hewlett-Packard Company
Regulator: Attorney General of the State of California

Basis for Complaint: The California AG filed civil and criminal complaints against HP and certain officers/directors for violations of various California laws. This case summary details the civil case, in which the AG alleged that HP used “false and fraudulent pretenses” (i.e., pretexting) to obtain confidential information (such as individual calling records and billing records) from a phone company in violation of CA Penal Code section 538.5.

The civil complaint also alleged HP violated Penal Code section 502(c)(2) by willfully and knowingly accessing, and without permission using, computerized telephone account data belonging to the victims. Additionally, the complaint alleged that HP violated California’s identity theft statute (Penal Code section 530.5) by willfully obtaining personal identifying information about the victims, then using that information for an unlawful purpose, according to the complaint. The claims in the civil case mirror those in the criminal filings.

Facts and Allegations: The cases arose as a result of actions taken by HP and third party investigators hired by HP to probe leaks of confidential board documents and discussions to the media. In the course of the investigation, phone records of various news reporters were obtained by false pretenses. Other information was obtained about the reporters, in an attempt to determine whether any reporters had access to insiders at HP who had divulged confidential information. The investigators also sought information about those HP board members who were suspected of sharing information with the reporters.

Although HP denied knowledge of the fact that the third party investigator had used false pretenses to obtain telephone records, the Chairman of the Board had authorized the investigation. In the wake of the scandal, the Chairman resigned. She was later charged with felony criminal counts related to the investigation, along with the HP ethics office and three of the private investigators. (California v. Dunn, Cal. Super. Ct., DA No. 061027481, 10/4/06). The civil complaint was filed shortly thereafter.

Outcome: HP settled the civil matter by agreeing to institute significant changes in its corporate governance processes, paying civil penalties and creating a Privacy and Piracy Fund to support enforcement efforts by the AG’s office.

With regard to corporate governance, HP agreed to:

- Establish an independent director to serve as the Board’s watchdog on compliance with ethical and legal requirements. The director will have specific responsibilities for carrying out oversight functions and reporting violations to the Board, other responsible HP officials and the Attorney General;

- Expand the oversight of its chief ethics and compliance officer (CECO). The CECO will review HP’s investigation practices and make recommendations to the Board and also report to the Board’s Audit Committee as well as to the General Counsel. Additionally, the CECO will have authority to retain independent legal advisors;

- Expand the duties of its chief privacy officer to include review of the firm’s investigation protocols to ensure they protect privacy and comply with ethical requirements;

- Establish a new Compliance Council, headed by the CECO, to develop and maintain policies and procedures governing HP’s ethics and compliance program; and
• Enhance its ethics and conflict-of-interest training and create a separate code of conduct, for use by outside investigators that addresses privacy and business ethics issues.

HP agreed to provide the AG with $13,500,000 to fund the Privacy and Piracy Fund. The Fund will be used to support law enforcement activities related to privacy and intellectual property rights. Additionally, HP agreed to pay $650,000 in civil penalties and $350,000 to cover the Attorney General’s investigation and other costs.

Note: settlement of the civil case did not affect the criminal cases that had been filed. One of the investigators pled guilty to charges; the court dismissed the charges against the HP Chairman and the investigators.

Fine Imposed: $14,500,000

III. Unfair Trade Practices

An unfair trade practice is defined as any commercial conduct that causes substantial injury that is not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition.xi

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 FTC 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, then 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."

THE GATEWAY LEARNING CASE (SEPTEMBER 2004)

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)

**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

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."

THE BJ’S WHOLESALE CLUB CASE (SEPTEMBER 2005)

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

IV. 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) xii and the Security Rule promulgated by the U.S. Department of Health and Human Services (“HHS”) under The Health Insurance Portability and Accountability Act of 1999 (“HIPAA”).

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

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.

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 or encryption. 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)

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 of $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.
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. 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)

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.
V. Marketing Communications

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.

Marketing communications are regulated globally. In the United States, Federal laws broadly regulate telemarketing and all forms of electronic communications (fax, email, and SMS/text messaging). The regulations include preference, content and process requirements. Additionally, these Federal laws generally do not preempt stricter state requirements, and many states have passed legislation regulating marketing communications that impose burdens greater than those required by Federal legislation.xv

Additionally, while no Federal or state laws generally limit direct mail, some types of direct mail communications are regulated. For example, Federal Trade Commission rules under the Fair Credit Reporting Act mandate an opt-out for pre-screened offers of credit or insurance. Some laws also regulate certain types of communications (such as pharmaceutical product marketing) regardless of medium.

Outside of the United States, other countries also regulate marketing communications, including electronic communications and direct mail. Countries with comprehensive data protection laws, such as Australia, Canada, and the European Union member states, require companies to obtain consent for any secondary use of personal information:

- **A secondary use** is any use of personal information other than as needed to fulfill the purpose for which it was collected. For example, if personal information is collected to process a sales transaction, the use of that information to send a marketing communication is a secondary use.

Given the pervasive nature of marketing, however, and the fact that marketing data is often generated without a primary use (such as when a marketing list is rented), data protection authorities often supplement the general rights provided by their privacy laws with specific legislation or regulation of targeted marketing.

Telemarketing

Telemarketing is a method of direct marketing where a seller (or its agent) engages in "a plan, program, or campaign . . . to induce the purchase of goods or services or a charitable contribution” using a telephone."

In the United States, telemarketing activities are regulated by the Federal Communications Commission and the Federal Trade Commission as well as by the states:

- **The Federal Communications Commission (“FCC”)** has issued regulationsxvi pursuant to the Telephone Consumer Protection Act (TCPA).

- **The Federal Trade Commission (“FTC”)** has issued its own Telemarketing Sales Rule (or TSR)xvii pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act.
Both of these regulations have existed since 1991, and both have been amended many times. For example, both The Telemarketing Sales Rule ("TSR") and The Telephone Consumer Protection Act ("TCPA") have been amended to accommodate (and regulate) new technology (such as automated/predictive dialers) and to implement the national Do-Not-Call ("DNC") Registry. Both the TSR and the TCPA impose preference, content and process requirements on telephonic communications. They also impose recordkeeping requirements on telemarketers.

The TSR and TCPA are both enforced aggressively by the Federal Trade Commission and Federal Communications Commission respectively. Violations of the TSR and TCPA can result in penalties of up to $11,000 per violation (i.e., each non-compliant call). Additionally, the TSR and TCPA do not generally preempt stricter state regulation of telemarketing. Approximately 43 states have enacted some form of telemarketing regulation. The state attorneys general enforce these laws, and many offer a private right of action as well.

**THE DIRECTV, INC. CASE (DECEMBER 2005)**

**Respondent:** DirecTV, Inc.

**Regulator:** Federal Trade Commission

**Basis for Complaint:** Violation of the Telemarketing Sales Rule

**Facts and Allegations:** Respondent is a California-based corporation that sells DirecTV satellite television programming to consumers throughout the U.S. and engages in telemarketing of its services to consumers. DirecTV entered into agreements with five telemarketing companies that made telemarketing calls on behalf of DirecTV.

The FTC complaint alleged that DirecTV violated the Telemarketing Sales Rule (TSR) by:

- Initiating (or causing other companies) to initiate calls to consumers whose numbers are registered with the National Do Not Call Registry;
- Abandoning (or causing other companies) to abandon calls to consumers by failing to connect a live sales representative within two seconds after the end of the consumer’s greeting; and
- Providing assistance to at least one telemarketer placing calls on its behalf while knowing or consciously avoiding knowing that the company was violating the TSR.

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

**TSR Compliance Program:** DirecTV shall develop, implement and maintain a well-documented and easily accessible system to receive and retain telemarketing-related complaints, with each complaint being promptly investigated. The system shall produce detailed monthly reports of telemarketing complaints that include complaints for each authorized telemarketer. For a period of three years after the order, DirecTV shall maintain a procedure of tracking the solicitation of new subscribers, identifying the authorized telemarketer responsible for the sale, and use the information to monitor compliance with the order.

DirecTV shall not violate the TSR directly or through its authorized telemarketers. DirecTV shall not:

1. Initiate any outbound telephone calls to consumers who requested not to receive calls;
(2) Initiate any outbound telephone calls to a number on the Federal Do Not Call Registry unless it has obtained express agreement in writing, has an established business relationship, or has met the provisions of the TSR Do Not Call safe harbor; or

(3) Abandon calls.

DirecTV is also permanently restrained from:

(1) Failing to conduct reasonable due diligence before making a person an authorized telemarketer;

(2) Failing to obtain a written contract with each authorized telemarketer, including the requirement that it comply with the TSR;

(3) Failing to monitor TSR compliance of authorized telemarketer campaigns and failure to discontinue business when the TSR is violated; and

(4) Providing substantial assistance to a telemarketer when it knows or consciously avoids knowing that the telemarketer is violating the TSR.

Maintenance of Relevant Documents: For a period of six years, DirecTV shall maintain and provide, within 30 days of request, any business records that demonstrate its compliance with this order.

Delivery of Order: For a period of three years after the order, and within five days of service of the order, DirecTV shall deliver a copy of the FTC order to all officers and directors, as well as employees having responsibility relating to telemarketing activities. The order shall be delivered to new employees before assuming responsibilities with DirecTV. In addition, it shall obtain a signed statement from each person acknowledging receipt of the order.

Reporting: For a period of three years, DirecTV shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Additionally:

(1) Within 30 days of a request by the FTC, DirecTV shall file additional reports, appear for deposition, or provide entry to any business location for FTC inspection;

(2) Within 180 days after service of order DirecTV shall file a report with the FTC setting forth its compliance with the order;

(3) Once every 12 months, after the initial 180 day report, and for three years thereafter, DirecTV shall file a report with the FTC detailing the monitoring activity of its authorized telemarketers;

(4) At the end of each quarter, after the initial 180 day report, and for 3 years thereafter, DirecTV shall file a report with the FTC describing all outbound telemarketing campaigns it conducted or that were conducted by its authorized telemarketers during the previous quarter; and

(5) Upon request of the FTC, DirecTV shall provide more detailed data for telemarketing campaigns.

Fine Imposed: $5,335,000 (When assessed, this was the largest civil money penalty imposed by the FTC in a telemarketing case.)
With the rise of “predictive dialers” in the late 1990s, consumers became very upset about the number of abandoned and “dead air” calls that they received. The Telemarketing Sales Rule was amended to address these issues. In particular, the TSR now places strict limits on the call abandonment rates, to help ensure that individuals are not harassed by automated telemarketing systems. The TSR requires companies to connect the consumers called to live operators within 2 seconds of the consumers’ completed greetings.

The Federal Trade Commission has opined that the use of pre-recorded marketing messages contravenes the call abandonment provisions because the pre-recorded message is not a live operator. According to the Federal Trade Commission’s “Complying with the Telemarketing Sales Rule” guidance (October 2005):

*Under the Rule’s definition, an outbound telephone call is “abandoned” if a person answers it and the telemarketer does not connect the call to a sales representative within two seconds of the person’s completed greeting.* The use of prerecorded message telemarketing, where a sales pitch begins with or is made entirely by a prerecorded message, violates the TSR because the telemarketer is not connecting the call to a sales representative within two seconds of the person’s completed greeting. (emphasis in original)

The Federal Trade Commission brings enforcement actions against companies that engage in pre-recorded message marketing.

**THE BROADCAST TEAM CASE (FEBRUARY 2007)**

**Respondent:** The Broadcast Team, Inc. (“TBT”) and various corporate officers

**Regulator:** Federal Trade Commission

**Basis for Complaint:** Violation of the Telemarketing Sales Rule (TSR)

**Facts and Allegations:** Respondent is a Florida-based telemarketer that sells a computerized “voice broadcasting” service that delivers prerecorded messages. This service, “RealCall”, uses automated dialers to initiate telephone calls. When a particular call is answered, a computerized system determines whether it has been answered by a live person, an answering machine or voicemail system. The service then delivers prerecorded messages to answering machines, voicemails and/or live people, depending on the particular programming applied. RealCall is capable of placing over one million such telephone calls each day.

The FTC complaint alleged that TBT violated the Telemarketing Sales Rule (TSR) by:

- Abandoning or causing others to abandon calls to consumers by failing to connect a live sales representative within two seconds after the end of the consumer’s greeting (over 64 million calls were abandoned since October 1, 2003, when answered by a live person instead of an answering machine or voicemail);

- Initiating calls between October 17, 2003 and January 15, 2004 to consumers whose numbers were registered on the Federal Do Not Call Registry (DNC Registry) and then continuing for several weeks after being instructed by its client to eliminate numbers that were listed on the DNC Registry; and
• Initiating calls on behalf of sellers who (advised by TBT that the fee was not required) had not first paid the required fee to access those numbers on the DNC Registry.

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

TBT shall not directly violate or cause others to violate the TSR. TBT shall not:

1. Fail to connect a live sales representative within two seconds after the call is answered by a person and greeting is completed, unless no more than 3% of all calls are abandoned per day, (for calls abandoned under the 3%, a recorded message stating the name and number of the seller must be played within 2 seconds of completed greeting whenever a sales representative is not available);

2. Initiate any outbound telephone calls to a number on the DNC Registry unless it is made to a business, to solicit charitable contributions, or to a person with whom TzbT has obtained express agreement in writing or has an established business relationship; and

3. Initiate any outbound telephone calls to numbers within areas without first paying the required annual fee to access the DNC Registry for that area.

**Maintenance of Relevant Documents:** For a period of five years, TBT shall maintain and provide, within 14 days of request, any business records that demonstrate its compliance with this order.

**Delivery of Order:** Within 30 days of service of the order, TBT shall deliver a copy of the FTC order to (and obtain signed statements from) all owners, principals, members, officers and directors, as well as employees and all others having decision making authority relating to the subject of the order. In addition, within 10 days of complying, TBT shall provide an affidavit setting forth its compliance with the order.

**Reporting:** TBT shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order. Additionally, for a period of five years, each individual defendant shall notify the FTC within 30 days of any employment or business affiliation changes that involve telemarketing responsibilities.

**Fine Imposed:** $2,800,000 ($1,000,000 payable within 5 days of order and the remainder suspended)

The Federal Trade Commission continues to make enforcement of the Telemarketing Sales Rule a priority. In November 2007, the Commission announced as many as six different settlements with companies alleged to have violated the TSR, including Craftmatic, ADT Security Services and two authorized security system dealers, and Ameriquest Mortgage Company. The settlements collectively imposed nearly $7.7 million in civil penalties.

The announcement also contained information on additional TSR cases that the Federal Trade Commission was filing against Guardian Communications (a company using prerecorded messages, similar to the Broadcast Team) and Global Mortgage Funding.

**THE CRAFTMATIC CASE (NOVEMBER 2007)**

**Respondent:** Craftmatic Industries, Inc. and its subsidiaries
Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Telemarketing Sales Rule

Facts and Allegations: Respondent is a Delaware corporation that sells adjustable beds and electronic mobility scooters through its subsidiaries (telemarketers) that call consumers to induce the purchase of its goods and services. Craftmatic ran sweepstakes promotions offering the chance to win a Craftmatic bed after filling out an entry form which indicated the consumers’ telephone number was also their entry number. The form did not indicate that by filing it out, they would receive sales calls. Craftmatic, without obtaining the consumers’ express consent, then used the information on the entry form to place calls to consumers.

The FTC complaint alleged that Craftmatic violated the Telemarketing Sales Rule (TSR) by:

- Initiating (or causing other companies) to initiate calls to consumers whose numbers are registered with the National Do Not Call Registry;
- Abandoning (or causing other companies) to abandon calls to consumers by failing to connect a sales representative within two seconds after the end of the consumer's greeting; and
- Initiating (or causing other companies) to initiate calls to consumers who previously requested not to receive calls from Craftmatic.

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

Craftmatic shall not directly violate or cause others to violating the TSR. Craftmatic shall not:

1. Initiate any outbound telephone calls to consumers who requested not to receive calls;

2. Initiate any outbound telephone calls to a number on the Federal Do Not Call Registry unless it has obtained express agreement in writing or has an established business relationship; or

3. Abandon calls by failing to connect a representative within two seconds of a person’s greeting unless (a) no more than 3% of all calls are abandoned per day, (b) the phone is allowed to ring for at least fifteen seconds or four rings before disconnecting the unanswered call, (c) a recorded message stating the name and number of the seller is played within two seconds of the completed greeting whenever a sales representative is not available, and (d) records establishing compliance are retained.

Maintenance of Relevant Documents: For a period of five years, Craftmatic shall maintain and provide, within 10 business days of request, any business records that demonstrate its compliance with this order.

Delivery of Order: Within thirty days of the entry of the Order, Craftmatic shall deliver a copy of the FTC Order to all owners, principals, members, officers and directors, as well as managers, agents, servants, employees and attorneys having decision-making authority relating to telemarketing activities. It shall obtain a signed statement from each person acknowledging receipt of the Order. In addition, within ten days of compliance, it shall file an affidavit setting forth its compliance.
**Reporting:** Craftmatic shall notify the FTC at least 30 days prior to any corporate change that may affect compliance with the order.

**Fine Imposed:** $4,400,000

As noted above, the Telemarketing Sales Rule and the Telephone Consumer Protection Act rules do not preempt state laws. Most states have laws that regulate telemarketing, and several states have their own no-call lists. These laws are enforced by state attorneys general or by individuals pursuant to a private right of action.

**THE MARKETLINKX CASE (DECEMBER 2007)**

**Respondent:** Marketlinkx Direct, a Florida telemarketer, and its owner, Ezell Brown

**Regulator:** Missouri State Attorney General

**Basis for Complaint:** Violation of Missouri state telemarketing laws and no-call list requirements

**Facts and Allegations:** Missouri attorney general sued the respondents after receiving numerous complaints of calls from Marketlinkx to consumers who had registered on the Missouri No-Call list.

**Outcome:** Marketlinkx and its owner entered into a voluntary assurance pursuant to which they agreed to cease calling Missourians on the No-Call list and otherwise comply with Missouri laws.

In addition to a fine, Respondents agreed to pay future civil penalties of up to $2,000 for violations of the assurance agreement and a $5,000 per violation penalty for any violations of state consumer protection laws.

**Fine Imposed:** $15,000

State telemarketing law enforcement is a priority for Missouri Attorney General, Jay Nixon and many of his counterparts in other states. In Missouri, for example, over 2.5 million people have registered on the state No-Call Registry.xx According to a story in the Branson Daily News, the Marketlinkx action brings the total collected from No-Call violators to $1,713,500 since July 2001.xxi The story notes that in July 2007, Mr. Nixon’s office fined a Florida mortgage broker $155,000 and a satellite TV marketing company $330,000.

Concerns about unsolicited calls and mobile phone marketing have prompted international regulators to take action against companies as well. Regulators in countries with established privacy laws frequently bring actions when companies fail to respect opt-out requests.

**Fax Communications**

The delivery of unsolicited marketing communications via facsimile is regulated under United States and international laws. Because fax transmissions are considered intrusive (often causing consumer phones to ring at night) and because recipients incur real costs in receiving faxes (such as costs associated with paper and machine cartridges), fax rules are generally well enforced.

In the United States, faxes are regulated by the Federal Communications Commission, under the Telephone Consumer Protection Act (discussed previously). The Federal Communications Commission ("FCC") enforces these rules. Several states also regulate fax communications under their own state telemarketing regimes. Because the TCPA does not preempt stronger state laws, the state fax rules often exceed the Federal Communications Commission's rules. For example, California law generally requires senders to have opt-in
consent to transmit marketing faxes. Approximately fifteen other states have similar opt-in rules for faxes.

In Canada, the telemarketing rules discussed above also regulate unsolicited commercial faxes. Canadian law requires opt-out consent for commercial faxes and imposes similar content regulations as with telemarketing.

### THE FAX.COM, INC. CASE (AUGUST 2002)

**Respondent:** Fax.com, Inc.

**Regulator:** Federal Communications Commission

**Basis for Complaint:** Violation of the Telephone Consumer Protection Act (TCPA)

**Facts and Allegations:** Respondent is a California-based corporation that operates as a “fax broadcaster”, sending messages to telephone facsimile machines on behalf of other entities for a fee. These messages advertise either the commercial availability or quality of a product, good or service and therefore constitute advertisements. Fax.com sent its clients’ advertisements using its own distribution list of facsimile numbers without verifying that the recipient had 1) consented to receive the fax or 2) had an established business relationship with Fax.com or its client. In addition, Fax.com did not disclose to its clients the prohibition regarding faxing unsolicited advertisements. The FCC issued citations in December 2000 and May 2001 informing Fax.com of its violations of the TCPA and that it could be subject to monetary forfeitures if it continues sending unsolicited facsimile advertisements.

The FCC Notice of Apparent Liability for Forfeiture alleged that Fax.com violated the Telephone Consumer Protection Act by:

- Sending unsolicited advertisements to telephone facsimile machines on 489 separate occasions;
- Not having an established business relationship with the consumer; and
- Not having prior written consent from the consumer for the faxes to be sent.

**Outcome:** By Order of Forfeiture to Fax.com, the FCC ordered Fax.com to come into compliance with the TCPA and the FCC’s rules and orders. It further ordered:

**Reporting:** Fax.com shall file a report with the FCC within 30 days of the Order indicating whether it has come into compliance with the TCPA and FCC rules prohibiting unsolicited advertisements to telephone facsimiles.

**Fine Imposed:** $5,379,000

### E-mail Communications

Concerns around unsolicited commercial email and spam have prompted many countries to enact laws regulating the transmission of unsolicited commercial email messages. These laws are generally well enforced globally.

In the United States, The Controlling the Assault of Non-Solicited Pornography and Marketing of 2003 (“CAN-SPAM”) regulates the transmission of commercial electronic mail messages. A commercial
electronic message is any email whose primary purpose is the advertisement or promotion of a commercial product, service or website. xxiii The CAN-SPAM Act is being implemented through regulations promulgated by the Federal Trade Commission and the Federal Communications Commission.

The CAN-SPAM Act imposes preference, content and process requirements on senders of commercial emails. The Federal Trade Commission, Federal Communications Commission, state attorneys general and Internet service providers bring actions to address CAN-SPAM Act violations.

**THE MEMBER SOURCE MEDIA CASE (JANUARY 2008)**

**Respondent:** Member Source Media LLC

**Regulator:** Federal Trade Commission

**Basis for Complaint:** Violation of the CAN SPAM Act; deceptive trade practices in violation of Section 5 of the FTC Act (see Chapter 2)

**Facts and Allegations:** Member Source operates the ConsumerGain.com, PremiumPerks.com, FreeRetailRewards.com, and GeatAmericanGiveaways.com, websites. Member Source used emails to attract consumers to these websites.

The FTC alleged that the Member Source emails were deceptive, in violation of the CAN SPAM Act and Section 5 of the FTC Act. For example, Member Source sent emails to consumers with subject lines such as "Congratulations. You’ve won an iPod Video Player"; "Here are 2 free iPod Nanos for You: confirm now"; "Nascar Tickets Package Winner"; "Confirmation required for your $500 Visa Gift Card"; or "Second Attempt: Target Gift Card Inside." Consumers that came to the websites saw similar statements, such as "CONGRATULATIONS! You Have Been Chosen To Receive a FREE GATEWAY LAPTOP." However, when consumers arrived at the Member Source websites, they were led through a series of ads for goods and services from third parties. To "qualify" for their "free products," consumers had to view pages of third party offers and "participate in" third party promotions by purchasing products, subscribing to satellite television service, or applying for credit cards.

The FTC alleged that, because consumers had to pay money and otherwise provide consideration to get the "free gifts" the subject lines in the Member Source emails were deceptive, in violation of the CAN SPAM Act. Additionally, because Member Source failed to disclose material facts, such as the fact that the consumers had to pay to obtain the "free products", its actions were deceptive in violation of the FTC Act.

**Outcome:** Member Source Media is permanently restrained and enjoined from:

(1) In any email and online advertisement, and on any landing page associated with such email or online advertisement, that contains any direct or implied representation made by Defendants, or made by any authorized agent on behalf of Defendants, that a product or service is free, failing to disclose, in the same color, font, and size, and within close proximity to such representation that a purchase is required, or that purchases are required, to obtain such product or service, when such is the case;

(2) On any landing page associated with any direct or implied representation made by Defendants, or made by any authorized agent on behalf of Defendants, that a product or service is free, failing to disclose, in a clear and conspicuous manner: (a) a list of the monetary obligations a consumer is likely to incur to obtain the advertised product or service, when such is the case;
(b) a list of any non-monetary obligations a consumer is likely to incur to obtain the advertised product or service, such as having to apply and qualify for credit cards or an automobile loan, when such is the case. (These disclosures may be made from such landing page via a hyperlink, provided that the hyperlink is labeled to convey the nature and relevance of the information to which it leads, and is clearly and conspicuously disclosed.); and

(3) Violating the CAN-SPAM Act including, but not limited to, by initiating the transmission of a commercial email message that misrepresents the content or subject matter of the message.

Record Keeping: For a period of eight (8) years, Member Source must create and retain:

(1) Accounting records that reflect the cost of goods or services sold, revenues generated, and the disbursement of such revenues;

(2) Personnel records accurately reflecting: the name, address, and telephone number of each person employed in any capacity by such business, including as an independent contractor; that person’s job title or position; the date upon which the person commenced work; and the date and reason for the person’s termination, if applicable;

(3) Customer files containing the names, addresses, phone numbers, dollar amounts paid, quantity of items or services purchased, and description of items or services purchased, to the extent such information is obtained in the ordinary course of business;

(4) Complaints and refund requests (whether received directly, indirectly or through any third party) and any responses to those complaints or requests; and E. Copies of all sales scripts, training materials, advertisements, or other marketing materials;

(5) Records demonstrating reasonable policies and procedures to process and handle customer inquiries and complaints;

(6) All records and documents necessary to demonstrate full compliance with each provision of this Order.

Fine Imposed: $200,000

VI. E-commerce and Online Activities

Many of the theories of liability applied to online activities have been discussed in the previous chapters. For example, deceptive trade practice cases have been brought as a result of corporate failure to live up to privacy promises made in posted website privacy notices. However, companies face particular risks associated with certain types of online behavior, such as delivery of content protection software and “adware” (advertising-supported, downloadable software) or the interaction with children online.

User-Installed Software

Companies concerned about protecting their intellectual property often rely on technology to prevent inappropriate copying of their content. These companies may require users to accept installation of digital rights management software to restrict use of content.
Other companies seek to capture information about users or to deliver content to users, such as advertising. These companies may encourage users to install software, perhaps to receive some type of free application, such as a screen saver, weather program or game.

United States trade practices laws require that the companies inform users about the software they are installing. Companies must also ensure that technology does not create security vulnerabilities for the users. Additionally, to the extent that the technology gathers personal information, it must do so in a way that is not deceptive.

THE SONY/BMG CASES (2006-2007)

**Respondent:** Sony BMG Music Entertainment, Inc. (Certain other parties, depending on the action)

**Regulators:**


**Case 2:** Texas State Attorney General (December 2006)

**Case 3:** Federal Trade Commission (June 2007)

Sony BMG was also sued in a number of private class action lawsuits in the US and Canada. Most of the US lawsuits were consolidated in the US District Court for the Southern District of New York and settled in December 2006 (the “New York Settlement”). The Canadian class actions were settled in September 2006.

**Basis for Complaints:**

**Case 1:** Violation of the various States’ consumer protection and trade practices statutes, e.g., Alabama Deceptive Trade Practices Act, Alaska Unfair Trade Practices and Consumer Protection Act

**Case 2:** Violations of the Texas Consumer Protection Against Spyware Act and the Texas Deceptive Trade Practices-Consumer Protection Act

**Case 3:** Unfair Trade Practices, Violation of Section 5 of the FTC Act

**Facts and Allegations:** Respondent distributes music compact discs ("CDs"). Sony BMG sold approximately 17.1 million music CDs to consumers that contained “MediaMax” and “Extended Copy Protection” (or XCP) digital rights management (“DRM”) software. When the CDs were played on consumers’ computers, the DRM software was subsequently downloaded and installed on the computers.

The various complaints and private lawsuits alleged that the DRM software was installed without appropriate notice to or consent of the users. Additionally the DRM software installed a potentially dangerous rootkit that rendered the computers vulnerable to malicious software and other security threats. In addition, the rootkit hid its existence from the Windows Operating System and in the process created a vulnerability that could allow third parties to access and gain full control over a consumer’s computer.
The various complaints also alleged that Sony did not appropriately notify users that the DRM software restricted the number of CD copies that can be made, limited the devices on which the music can be played, and contained technology that, undisclosed to consumers, monitors their listening habits in order to send marketing messages.

Finally, the complaints alleged that Sony made the DRM software difficult to locate and remove from users’ computers.

**Outcome:** As part of the New York Settlements, Sony BMG agreed to strong restrictions on its use of DRM software going forward. Under this agreement Sony BMG agreed that if it manufactured any CDs with any DRM software from the settlement date through December 31, 2007, it will:

1. Ensure that the DRM software operates in a manner ensuring that no software will be installed on the hard disk drive of a user’s computer unless and until the user has agreed to such installation by accepting an End User License Agreement ("EULA") or by otherwise affirmatively consenting to such installation.

2. Ensure that an uninstaller for such DRM software is made readily available to consumers, without their needing to provide personal information, either on the CD, through a link on the CD’s user interface, or by such other comparable method as is generally used in the software industry.

3. Ensure that the functionality of any updates and/or material changes in functionality of the DRM software is adequately disclosed.

4. Ensure that any EULA associated with the DRM software accurately describes the nature and function of the software, and does so in easily understandable language.

5. Show any EULA associated with the DRM software in advance of its use to an independent third party (the “EULA Reviewer”) to be designated jointly by Sony BMG and Plaintiffs’ Class Counsel, and receive comments on the proposed EULA from the EULA Reviewer. Sony BMG shall consider, but will not be required to adopt, the comments of the EULA Reviewer. However, to the extent that Sony BMG determines not to accept the EULA Reviewer’s comments, the EULA Reviewer will not be required to keep such non-accepted comments confidential.

6. Provide any DRM software to at least one qualified, independent third party, and obtain an opinion from that third party that the installation and use of the software would create no confirmed security vulnerabilities.

7. Ensure that, with respect to CDs with DRM software, Sony BMG will, if such CDs are played on computers with active connections to the Internet and the CDs cause the computer to make a connection to the Internet, make a record only of the associated album title, artist, IP address from which the connection was made, and certain non-personally identifiable information; provided, however, that the foregoing shall not preclude Sony BMG from obtaining personally-identifiable information from the user upon consent.

8. Include, on any Sony BMG CD containing any DRM software, a written disclosure, in plain language and type size, and at a location reasonably calculated to provide appropriate pre-sale notice to consumers, that the CD contains such DRM software and a brief description of such
DRM software, and, unless such connection is only made upon the user’s prior informed, affirmative consent, that the CD seeks to connect to a Sony BMG (or a contractor’s) server.

(9) If the Sony BMG personnel responsible for DRM software are made aware of a suspected security vulnerability, either by virtue of their weekly monitoring of a designated email address or other designated means of communication, or otherwise, it will take the following steps:

(a) Sony BMG will ensure that, within no more than five (5) business days after having received such notice, the circumstances of the suspected security vulnerability are communicated to the security expert for evaluation and testing.

(b) If the security expert determines that the suspected security vulnerability is a confirmed security vulnerability (which determination will be made as soon as practicable), within five (5) business days after the vulnerability is confirmed Sony BMG will, to the extent practicable and where appropriate, notify at least two major computer security providers (e.g., Symantec and Microsoft) of the confirmed security vulnerability.

(c) As soon as practicable, and, in any event, within thirty (30) days after the determination that there is a confirmed security vulnerability, Sony BMG will cause to be developed and released an update to the DRM software that corrects the confirmed security vulnerability. The thirty (30)-day period may be extended for good cause if an update is under development, and Sony BMG believes that an update will be able to be released within a reasonable time.

(d) When Sony BMG releases such an update, it will, to the extent practicable, notify at least two major computer security providers (e.g., Symantec and Microsoft) of the update. The update shall remain continuously available on or through Sony BMG’s website throughout the Injunctive Period.

(e) When Sony BMG releases such an update, it will also notify Plaintiffs’ Class Counsel.

(f) If, after the period specified above in subparagraph (c), Sony BMG determines that it cannot effectively address the confirmed security vulnerability through means of an update, it will notify Plaintiffs’ Class Counsel, and will meet and confer with Plaintiffs’ Class Counsel on an appropriate course of action. Sony BMG will take such action as it deems appropriate. If Plaintiffs’ Class Counsel does not believe that the actions taken by Sony BMG are appropriate, it may seek relief from the Court, pursuant to the Court’s continuing jurisdiction over matters related to this Settlement Agreement.

Additionally, in its other agreements with the Regulators, Sony BMG further agreed:

(1) Sony BMG’s product packaging shall clearly and prominently disclose details about any software bundled with CDs (i.e. that it will install on consumers’ computers, limit the number of copies that can be made, limit the transfer of files to certain Windows or Sony format devices, and that declining to install it will prevent consumers from accessing or listening to the audio files on their computer).

(2) Sony BMG shall not install any DRM software on consumers’ computers without: (a) properly disclosing on the computer screen the information required above; (b) clearly and prominently disclosing on the consumers’ computer screen that declining to install the DRM software will prevent them from accessing or listening to their audio files on computers; and (c) obtaining consumers’ assent to install the software by clicking a clearly labeled button/link.
(3) Sony BMG shall not use any information it collected from the Internet about its consumers for marketing purposes or to deliver marketing messages. It shall destroy all such data within three days of receipt.

(4) Prior to transmitting consumer information via the internet Sony BMG shall (a) clearly and prominently disclose on the computer screen that this information will be transmitted back to Sony BMG, and (b) obtain the consumer’s assent to transmit the information.

(5) Sony BMG shall not install any DRM software that prevents consumers from easily locating and/or removing the software and shall provide a reasonable and effective means to uninstall the software.

(6) Sony BMG shall:

- For a period of two years after the order, provide, free of charge, a program and patch that uninstalls XCP and MediaMax software and removes the associated security vulnerability;

- For a period of two years after the order, post a notice on its website containing information about the uninstall programs and security patch; and

- For a period of 12 months after the order, continue purchasing Internet browser premium keywords to give consumers notice of the security vulnerability associated with the DRM software and the steps to take to protect their computers.

(7) Sony BMG shall extend for 180 days the exchange and compensation program outlined in [the New York Settlement agreement]. It shall also post notices on its website about the extended program and about the repair reimbursement program (see Fines Imposed section below).

**Fines Imposed:** Pay up to $150 in consumer redress to each affected consumer to repair damage to their computers caused by Sony BMG’s software, as provided in the New York Court settlement.

**Case 1:** $4,250,000 to the States

**Case 2:** $750,000 to the State of Texas

(No additional fine imposed by the FTC)

---

**THE DIRECTREVENUE CASE (JUNE 2007)**

**Respondent:** DirectRevenue, LLC

**Regulator:** Federal Trade Commission

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

**Facts and Allegations:** Respondent is a large software distributor that conducts business principally out of New York. DirectRevenue developed, downloaded and installed advertising-
supported software ("adware") to consumers’ computers, both directly and through affiliates. The consumers were often unaware of the adware installation, as it was frequently bundled together with other free or paid software programs.

This adware tracked and stored information regarding consumers’ internet usage, and then used that information to personalize and display pop-up and other advertisements directly on consumers’ computers. DirectRevenue also made it very difficult for consumers to locate and remove the adware by using names that resemble core system software or programs, keeping it off the add/remove programs utility, and other practices.

In light of the activities listed above, the FTC complaint alleged that DirectRevenue violated the FTC Act by:

- Deceptively failing to disclose adware bundled together with other software;
- Unfairly installing adware on consumers’ computers; and
- Using unfair uninstall practices related to the adware it had installed.

The FTC classified this conduct as deceptive and unfair under Section 5(a) of the FTC Act as the violations caused substantial injury to consumers.

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

DirectRevenue shall establish, implement and maintain a comprehensive program that is reasonably designed to ensure that its affiliates obtain express consent before installing DirectRevenue’s programs or applications onto consumers’ computers. This program shall include:

1. Obtaining contact information from prospective participants in any affiliate program;
2. Providing potential affiliates with a copy of the order and written notice that violation of the order will result in immediate termination of the affiliate program account. In addition, a signed and dated statement shall be obtained acknowledging receipt of and agreement to comply with order;
3. Requiring each affiliate program to provide identifying information of its sub-affiliates, employees, agents, sub-contractors or anyone else whose work corresponds to the subject matter of this order. In addition, each person listed above shall receive a copy of the order and shall provide a signed and dated statement acknowledging receipt of and agreement to comply with the order;
4. Establishing, implementing and maintaining a functioning email address or other Internet-based mechanism to report consumers’ complaints (regarding the practices of DirectRevenue or of its affiliates), and clearly and prominently disclosing that mechanism on DirectRevenue’s websites. In addition, DirectRevenue shall associate complaints with the appropriate software, application, website, good or service (or with the appropriate affiliate program when applicable) and respond to complaints in a timely manner via email or other Internet-based mechanism;
5. Investigating promptly and completely the complaints received in order to determine if any participant affiliate is engaging in acts or practices that violate the order;
(6) Terminating any affiliate that has violated this order, and immediately ceasing to display
advertisements or send any communications to the consumers who received software through
the violations of the affiliate; and

(7) Identifying clearly and prominently the program causing the display of any advertisement,
along with providing a hyperlink to a webpage that gives clear and prominent instructions for
uninstalling the software or application and accessing DirectRevenue’s complaint mechanism.

DirectRevenue shall not send advertisements or other communications through any program or
application it installed on consumers’ computers prior to October 1, 2005. Within 30 days of the
order, DirectRevenue may send up to 3 notices to these consumers’ computers advising them that
they will no longer receive advertising or communication from DirectRevenue and further advising
them as to how they may either authorize DirectRevenue to continue sending advertisements or
how they may remove the programs or applications from their computers. DirectRevenue shall not:

(1) Install, publish or otherwise distribute any software script, code, program, or other content that
exploits security vulnerabilities on any computer operating system, web browser, or other
application in order to download or install any software script, code, program or content onto
any computer;

(2) Download or install any software program or application without express consent to do so; or

(3) Install any program or application unless it provides consumers with reasonable and effective
means to uninstall the same.

Maintenance of Relevant Documents: For a period of five years from the order, DirectRevenue
shall maintain and provide upon request a print or electronic copy of any document that
contradicts, qualifies, or calls into question DirectRevenue’s compliance with the order.

Delivery of Order: DirectRevenue shall deliver a copy of the order to all current and future
principals, officers, directors, and managers and to all current and future employees, agents and
representatives who have responsibility over the subject matter of the order within 30 days. The
order shall be delivered to new employees within 30 days of assuming responsibilities with
DirectRevenue.

Reporting: DirectRevenue shall notify the FTC at least 30 days prior to any corporate change (or
proposed change) that may affect compliance with the order. Within 60 days after service of the
order and when required by the FTC, DirectRevenue shall file a report setting forth its compliance
with the order. It shall also cooperate with the FTC after written notice and appear, or cause
officers, employees, representatives or agents to appear for interviews, conferences, discovery,
review of documents, testimony, deposition or any other matter or proceeding relevant to the
subject of the order.

Fine Imposed: $1,500,000

The New York Attorney General addressed DirectRevenue’s conduct by bringing enforcement actions against
companies that engaged DirectRevenue as an adware marketing partner.
THE INTERNET ADVERTISERS CASE (JANUARY 2007)

Respondents: Cingular Wireless LLC, Travelocity.com LP, Priceline.com Incorporated

Regulator: New York State Attorney General

Basis for Complaint: Violation of NY General Business Law – deceptive trade practices

Facts and Allegations: As described in the DirectRevenue case summary above, DirectRevenue developed, downloaded and installed advertising-supported software (“adware”) to consumers’ computers. The adware then delivered a steady stream of advertisements for DirectRevenue’s customers to the consumers when they surfed the Internet. The consumers were often unaware of the adware installation, as it was frequently bundled together with other free or paid software programs.

The respondents were clients of DirectRevenue LLC; they engaged DirectRevenue to deliver ads for their websites and services to Internet users who had downloaded the DirectRevenue software. The Attorney General alleged that the respondents each knew that consumers downloaded the adware without full notice and consent. The Attorney General further alleged that, by using DirectRevenue’s adware to advertise their products and services on the Internet, the respondents engaged in a deceptive business practice, in violation of New York law.

Outcome: Each of the respondents voluntarily entered into an Assurance of Discontinuance Agreement with the AG to settle the claims. Each agreement requires the respondent, if it uses adware in the future to:

(1) Require its adware marketing partners to agree in writing to:

- Provide consumers with full disclosure of (i) the name of each company delivering its advertisements through adware, (ii) the name of the adware programs, and (iii) the name of all software bundled with the adware programs;

- Brand each advertisement with a prominently and easily identifiable brand name or icon, and use the branding consistent with each advertisement attributable to the brand;

- On each screen and dialog box (without having to scroll down) where adware or bundled software is offered, provide a description of the adware’s functions, identify all information monitored, stored and/or distributed by the adware program and obtain consumer consent to both download and run the adware;

- Provide a conspicuous entry in the Add/Remove Programs facility in the consumer’s operating system that identifies the adware brand and provider, and does not require consumers to download any additional applications to complete the uninstallation; and

- For all consumers who previously downloaded the adware, provide notice that meets the requirements above and obtain consent to continue serving ads to these consumers.

(2) Implement a due diligence program with respect to adware advertising, with such due diligence performed at inception of a relationship and quarterly thereafter, whereby the respondent shall:
• Ask its adware marketing partners to provide the names of all programs used by the companies to deliver its advertisements;

• Download each of the identified adware programs at a sampling of three websites obtained through independent Internet research;

• Verify that the adware programs comply with the Assurance and company policy; and

• Cease using any adware program that violates this assurance or company policy.

(3) Within 30 days and annually for the next three years, provide a certified letter or affidavit to the Attorney General’s office setting forth its compliance with the terms.

**Fine Imposed:** $35,000 against Priceline.com, 
$30,000 against Travelocity 
$35,000 against Cingular Wireless

The agreements in these cases strongly suggest that companies who seek to use digital rights management software, adware or other tools should take steps to ensure transparency of any process that installs software or otherwise changes a user’s computer state. The functionality of the software must be clearly disclosed as well. Transparency should be obtained by including information on the company websites, on product packaging, and in clearly-written end user agreements that are presented to users in a conspicuous manner prior to installation.

Consumer protection and fair trade practices laws likely also require companies to:

• Obtain consent to digital rights management (“DRM”) software or adware installation or computer state changes. If the software collects personal information, companies obtain specific consent for this data collection as well;

• Provide a readily-available uninstaller for installed software free of charge; and,

• Take appropriate and reasonable steps to ensure that the software does not create any security vulnerabilities for the users. If vulnerabilities are later discovered, take immediate and appropriate steps to protect users from possible threat (such as notifying security companies and the users).

**Social Networking Web sites**

Significant concerns have been raised by regulators about privacy and consumer protection in the context of social networking Web sites. While The Children’s Online Privacy Protection Act of 2000 (“COPPA”) restricts the ability of commercial website operators in the United States to collect personal information of children under thirteen years of age,xxiv teens have passionately embraced social networking and shown little discretion in the posting of personal information. As a result of high-profile cases of pedophiles accessing teen profiles, contacting the teens and abusing them, the state attorneys general began investigating the major social networking website operators.

**THE FACEBOOK CASE (OCTOBER 2007)**
Respondent: Facebook Inc., dba as Facebook.com

Regulator: New York State Attorney General

Basis for Complaint: Violation of NY General Business Law – deceptive trade practices

Facts and Allegations: Facebook is a social networking website that allows individuals (including teenagers) to create a free profile, post personal information and pictures, and link to friends’ profiles.

The NY AG alleged that Facebook made misrepresentations about its website by claiming that children on Facebook were safer from sexual predators than at most sites, and by claiming that it promptly responds to safety concerns. Facebook had also represented itself as a “trusted environment for people to interact safely” and a website invested heavily in “building safety controls.”

The AG alleged that Facebook’s security controls had serious deficiencies. In particular, the AG alleged that investigators, “posing as young teenagers, set up profiles on Facebook, received online sexual advances from adults within days, and found widespread pornographic and obscene content.” Additionally, the AG alleged that “Facebook often failed to respond, and at other times was slow to respond to complaints lodged by the investigators - posing as parents of underage users - asking the site to take action against predators that had harassed their children.”

Outcome: Facebook voluntarily entered into an Assurance of Discontinuance Agreement with the AG to settle the claims. This agreement requires Facebook to:

(1) Disclose newly implemented safety procedures on its website as specified by the agreement;

(2) Accept complaints about nudity or pornography, harassment or unwelcome contact confidentially or via an independent email to abuse@facebook.com;

(3) Respond to and begin addressing complaints about nudity or pornography, harassment or unwelcome contact within 24 hours;

(4) Retain an Independent Safety and Security Examiner (ISSE) approved by the AG for 2 years;

(5) Allow Facebook’s complaint review process to be examined by the ISSE;

(6) Provide users and non-users (such as the parents and guardians of users) with easy online access to the ISSE; and

(7) Submit to the AG reports prepared by the ISSE evaluating Facebook’s performance in responding to complaints.

Fine Imposed: None

THE MYSPACE CASE (JANUARY 2008)

Respondent: MySpace

Basis for Complaint: The settlement culminated a 2 year investigation by the AGs into the use of MySpace by children and the risks presented to children by the social networking environment.

Facts and Allegations: The AGs alleged that MySpace did not have appropriate controls to verify and authenticate participants in the social networking website. They further alleged that MySpace did not taken sufficient steps to protect children from inappropriate content and adult predators on the site.

Outcome: The AGs and MySpace published a Joint Statement on Key Principles of Social Networking Sites. xxv

The AGs and MySpace reached a voluntary agreement containing the following provisions:

(1) MySpace will make web site design and functionality changes to better protect children from adult contact and content. For example, MySpace agreed to change profile settings for users under age 18, so that profiles of 14 and 15-year olds were automatically private and the profiles of 16 and 17-year olds were private by default.

(2) MySpace will create and lead an Internet Safety Technical Task Force, with support from the AGs, to develop age and identity verification tools for social networking sites. This Task Force will collaborate with other social networking site operators, identify verification experts, child protection groups and technology companies.

(3) MySpace will hire a contractor to create a registry of email addresses associated with children whose parents want to restrict their access to the site. MySpace will prohibit individuals using these registered email addresses from creating a profile.

(4) MySpace agreed to:
- Strengthen software identifying underage users;
- Retain a contractor to better identify and expunge inappropriate images;
- Obtain and constantly update a list of pornographic web sites and regularly sever any links between them and MySpace;
- Implement changes making it harder for adults to contact children;
- Dedicate meaningful resources to educating children and parents about on-line safety;
- Provide a way to report abuse on every page that contains content, and consider adopting a common mechanism to report abuse and respond quickly to abuse reports; and
- Create a closed "high school" section for users under 18.

(5) MySpace also agreed to work to increase its educational efforts, by providing information and tools for parents, educators and children about Internet safety. It agreed to support AG efforts to improve law enforcement ability to investigate and prosecute Internet crimes.

Fine Imposed: None
Personal Information of Children

The Children’s Online Privacy Protection Act of 2000 (“COPPA”) regulates the collection of personal information of children under 13 by commercial website operators. The Federal Trade Commission has promulgated rules to implement COPPA, and it frequently brings actions against companies that have not complied with the COPPA requirements.

THE HERSHEY CASE (FEBRUARY 2003)

Respondent: The Hershey Company

Regulator: Federal Trade Commission

Basis for Complaint: Violations of the Children’s Online Privacy Protection Act of 1998 and Section 5 of the FTC Act

Facts and Allegations: Respondent is the maker and marketer of chocolate and confectionary products including the popular Mounds, Reese’s, and KitKat brands. The company offered a special section on its corporate website directed at children under the age of 13. Known as “Kidztown”, this section featured children’s games, cartoon characters, and a “Candy of the Month” promotion. Hershey collected children’s personal information from this portion of the website including: name, address, email address, gender, approximate age, and often telephone number. Hershey also marketed a number of its products through individual websites dedicated to each candy brand. These websites similarly targeted and collected information from visitors including children.

Hershey and its affiliate branded websites managed a sweepstakes to give away free candy. Registration required parental consent. The parental consent form only required the name, home address, and the selection of the “I consent” box. Additionally, even if no information was entered in the parental forms and the child had indicated that he/she was under age 13, Hershey still accepted the registration. Sweepstakes winners' names and home states were published on the website without parental consent.

The FTC alleged that, in violation of COPPA and Section 5 of the FTC Act, Hershey operated a Web site directed at children and had actual knowledge that it collected personal information from children without sufficient parental consent, notice on its website, direct notice to parents of the information collected, and without providing reasonable means for parents to review/delete the information.

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

Bar on Misrepresentation: Must fully disclose information collection, use, and disclosure policies on the website and in direct parental notice.

Treatment of the Children’s Personal Information: Hershey shall, within five days of the Consent Decree date, delete all personal information collected from children through its websites (other than information collected in compliance with COPPA).

Consumer Education Remedy: For five years, Hershey shall place a clear and conspicuous COPPA notice on its websites (within its privacy policy) and within the direct notice required to be sent to parents in boldface type directing them to the privacy policy statement online.
Maintenance of Relevant Documents: For a period of five years, Hershey shall provide (upon request):

1. A copy of its different information collection forms;
2. Collection, use, and disclosure policies with regard to children; and
3. Any document that contradicts, qualifies or questions Hershey’s compliance with the order.

Delivery of Order: Within 30 days, Hershey shall deliver and obtain signed receipt of the FTC order along with the FTC compliance guide entitled “How to Comply with the Children’s Online Privacy Protection Rule” with respect to each current (and for three years, future) director, employee, agent, representative, or employee with managerial responsibility.

Reporting: For 20 years, Hershey shall notify the FTC within 30 days of any change which may affect its compliance with the order. Within 120 days after service of order and thereafter as requested, Hershey shall file a report with the FTC setting forth its compliance with the order including:

1. Information collection practices;
2. Copy of different privacy notice on websites;
3. Copy of parental privacy notices;
4. How to obtain parental consent;
5. How to provide opportunity for parents to review information collected; and

Fine Imposed: $85,000

The Xanga case demonstrates the Federal Trade Commission’s application of the COPPA rules to the operation of social networking sites that attract children.

THE XANGA CASE (SEPTEMBER 2006)

Respondent: Xanga.com, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violations of the Children’s Online Privacy Protection Act of 1998 and Section 5 of the FTC Act

Facts and Allegations: Respondent is a social networking website that was started in 1999 and is based in New York City. In 2005 it had approximately 25 million registered accounts. Xanga users are required to set up a personal profile which then allows them to post information about themselves and create personal pages or blogs containing profile information such as online journals, images, text, videos, etc. These profiles and personal pages are available for other users to read and respond to, and are also available to the general public through global search engines such as Google and Yahoo.

Xanga’s website terms of use policy stated that children under age 13 could not join. However, over a period of five years, Xanga created 1.7 million accounts for (and collected and disclosed personal information from) users who indicated they were under age 13.
The FTC alleged that Xanga violated the Children’s Online Privacy and Protection Act, the COPPA Rule and the FTC Act by knowingly collecting personal information from children under the age of 13 and by failing to:

(1) Provide notice to parents of information collection practices;

(2) Obtain parental consent prior to collecting, using & disclosing children’s personal information online; and

(3) Provide parents with reasonable means to access and control their children’s information.

**Outcome:** The FTC entered into a consent decree with Xanga, ordering that all websites and online services operated by Xanga and its principals shall comply with COPPA and applicable FTC Rules. Additionally, within five days from the entry of the Consent Decree, Xanga shall delete all personal information collected and maintained in violation of COPPA through the date of the order.

For five years, Xanga shall place on its homepage(s) and privacy notice(s) a clear and conspicuous notice in boldface type regarding the FTC’s program for protecting children, along with a hyperlink to the FTC’s website. An additional notice to parents regarding children and social networking sites must be included:

(1) Within the privacy policy required to be posted on its website;

(2) Within the direct notice required to be sent to parents in boldface type directing them to the privacy policy statement online; and

(3) In boldface type and in the form of a hyperlink at each location on its website(s) that collects personal information.

**Maintenance of Relevant Documents:** For a period of five years, Xanga shall provide (upon request and within 14 days) all documents demonstrating compliance with the terms and provisions of the Consent Decree.

**Delivery of Order:** Within 30 days, Xanga shall deliver and obtain a signed receipt of both the FTC order and the FTC COPPA compliance guide with respect to each of the principals, officers, directors, and managers, and to all employees, agents, and representatives having responsibilities related to this order; a list of these names should be submitted to the FTC within 10 days of complying with the order along with a statement setting forth its compliance. Delivery of the same is required for five years to all future directors, officers, agents, and managerial employees.

**Reporting:** For 3 years, the FTC shall be notified (1) by the individual defendants within 10 days of any changes in addresses or telephone numbers, employment or business ownership, or names and aliases; and (2) by Xanga 30 days prior to any changes in corporate structure which may affect its compliance with the order.

Within 60 days after service of the order and thereafter as requested, Xanga and the other individual defendants shall file reports with the FTC setting forth their compliance with the order including:

(1) Current residential and businesses addresses and telephone numbers, and descriptions of business activities and responsibilities of the individual defendants;
(2) Statement of website registration criteria and process, and copies of pages that provide/collect registration information;  

(3) Copy of all privacy notices posted on Xanga’s websites, and a statement detailing the location of the notices along with copies of the pages that collect personal information;  

(4) Copy of all privacy notices sent to parents, and a statement detailing when and how the notices were provided;  

(5) Statement detailing the methods used to obtain parental consent prior to the collection and use of children’s personal information;  

(6) Statement detailing the means provided for parents to access and control their children’s personal information;  

(7) Statement detailing the reasonable necessity for collecting each type of information from a child; and  

(8) Statement detailing the procedures used to protect the personal information collected from children.  

Fine Imposed: $1,000,000

State attorneys general also can bring COPPA actions as evidenced by the Santa.com case, below.

### THE SANTA.COM CASE (DECEMBER 2007)

**Respondent:** Small’s Seed Company, LLC  

**Regulators:** Texas State Attorney General  

**Basis for Complaint:** Violations of the Texas Deceptive Trade Practices-Consumer Protection Act and the Children’s Online Privacy Protection Act (COPPA)  

**Facts and Allegations:** Respondent maintains a website “Santa.com” that allowed children to make Christmas wish lists, write e-mails to Santa, play games, and read blogs from Santa and his reindeer, among other things. The Texas Attorney General alleged that the website collected personal information from children under 13 years of age in violation of COPPA. The Texas Attorney General also alleged that the respondent made false, deceptive or misleading statements about its collection of information from children on the website and failed to clearly and conspicuously disclose all material information regarding its information collection practice, as required by the Texas Deceptive Trade Practice law.  

**Outcome:** Although respondent denied the allegations above, it agreed to enter into an Assurance of Voluntary Compliance, providing that it will:  

(1) Make no misrepresentation regarding its information handling practices;
(2) Comply with COPPA, by (for example) providing COPPA-required notices on its home page and those pages that collect personal information from children under 13, obtaining verifiable parental consent prior to collecting information from such children, and not requiring such children to provide personal information except as necessary to participate in the activities offered; and

(3) Delete any information collected previously from children under 13 in a way that did not comply with COPPA.

Fine Imposed: None

Consumer Reporting Data and Credit Information

The Fair Credit Reporting Act ("FCRA") regulates the collection, disclosure and use of any third-party information used to make decisions about consumers' eligibility for credit, insurance, employment, government benefits and other purposes, such as residential housing.

The Federal Trade Commission has promulgated rules to implement the Fair Credit Reporting Act as applied to consumer reporting agencies, users of consumer reports and entities that furnish data to consumer reporting agencies.

Financial institutions outside of the Federal Trade Commission's jurisdictions receive FCRA compliance oversight from their Federal financial institution regulators. The FCRA is also enforced by state attorneys general, state insurance company regulators, and through private lawsuits.

THE CHOICEPOINT CASE (JANUARY 2006)

Respondent: ChoicePoint, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violation of the Fair Credit Reporting Act (FCRA)

Facts and Allegations: Respondent is a Georgia-based data broker that collects and sells consumer reports and other consumer data to businesses, professionals and government agencies that use the data for risk management, FCRA permissible purposes such as insurance underwriting and employment, and other purposes. These entities must apply to become ChoicePoint subscribers. The applications are processed in order to establish that the applicant is a legitimate organization and has an appropriate, permissible purpose for purchasing the consumer data. Once the applicant is approved as a subscriber, it may access consumer data from ChoicePoint, including consumer reports.

In early 2004, ChoicePoint discovered that sensitive personal information of approximately 145,000 consumers had been disclosed to persons who lacked a proper purpose to obtain such information. According to the FTC, the information was obtained by criminals who had posed as legitimate business and been approved as subscribers based on applications containing false information and other misrepresentations.
The FTC alleged that ChoicePoint failed to have reasonable procedures in place to screen potential subscribers, causing it to fail to detect the false information and other misrepresentations in the applications. As a result, ChoicePoint violated the Fair Credit Reporting Act by:

- Furnishing consumer reports to subscribers who did not have a permissible purpose;
- Failing to first make a reasonable effort to verify the identity of the prospective user and its intended uses of the consumer reports;
- Continuing to furnish consumer reports when it had reasonable grounds for believing the consumer reports would not be used for a permissible purpose; and
- Failing to monitor and identify unauthorized activity after being alerted of fraudulent activity from authorities between 2001 and 2005.

The FTC alleged that ChoicePoint also violated the FTC Act by failing to use reasonable and appropriate measures to protect the security of sensitive personal information and that this failure caused or is likely to cause substantial injury to consumers. The FTC classified these acts and practices as unfair or deceptive under Section 5 of the FTC Act.

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

Bar on Misrepresentation: ChoicePoint shall not misrepresent the manner or extent to which it maintains and protects the privacy, confidentiality or security of the personal information it collects.

FCRA-related Provisions: ChoicePoint is permanently restrained from furnishing consumer reports to persons who do not have a permissible purpose; therefore it must maintain reasonable procedures to ensure that consumer reports are provided only to those with a permissible purpose. These procedures include (1) obtaining written certification from each subscriber describing the nature of its business and specific intended permissible purpose for using consumer data, (2) verifying the subscribers’ identity and the legitimacy of its business, and (3) determining whether each subscriber has a permissible purpose. In addition, ChoicePoint shall alert its subscribers to the penalties for violating FCRA.

Security Program: ChoicePoint 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 the 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 identify risks; and
(4) Evaluation and adjustment of the information security program according to assessment and any material changes in the business.

Third Party Audit: Within 180 days after service of order and thereafter biannually for twenty years, ChoicePoint must obtain an assessment and report from an independent, third party within 60 days after the end of the reporting period that:

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

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

Maintenance of Relevant Documents: For a period of six years, ChoicePoint shall create and retain the following:

(1) Subscriber files containing all materials used to verify the identity of subscribers;

(2) Consumer complaints and responses to complaints;

(3) Copies of all training materials;

(4) Copies of all subpoenas and communications with law enforcement personnel; and

(5) Copies of all records or documents that show full compliance with the order.

For a period of three years after the preparation of each biennial assessment, ChoicePoint shall retain all plans, reports, studies, reviews, audits, audit trails, policies, training materials, work papers and assessments.

Delivery of Order: For a period of five years after service of the order, ChoicePoint shall deliver a copy of the FTC order to all officers, directors, and managers who have responsibility related to this order. Within ten days after service of order, ChoicePoint shall deliver an accurate summary of the order to all current employees who are engaged in conduct related to ChoicePoint’s compliance with the order or the required information security program and assessments. Future employees engaging in the above conduct should receive the summary no later than the date they assume job responsibilities. ChoicePoint shall obtain signed and dated statements acknowledging receipt of the order from each person.

Reporting: For a period of 20 years after service of the order, ChoicePoint 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 the order and thereafter as requested, ChoicePoint shall file a report with the FTC setting forth its compliance with the order.

Fine Imposed: $10,000,000 in civil penalties plus an additional $5,000,000 that the FTC used to create a fund for consumer redress.

The FCRA also imposes process requirements on consumer reporting agencies, companies that furnish data to the consumer reporting agencies and users of consumer reports. For example, under the Fair Credit Reporting Act, companies that use consumer reports must provide individuals with notice when information in a consumer report is used in whole or in part to make an adverse decision. The Federal Trade Commission and state attorneys general can bring actions to enforce the adverse action notice requirements of the FCRA.
THE QUICKEN LOANS CASE (DECEMBER 2002)

Respondent: Quicken Loans, Inc.

Regulator: Federal Trade Commission

Basis for Complaint: Violation of Fair Credit Reporting Act

Facts and Allegations: The FTC alleged that Quicken Loans, a Michigan-based mortgage lender, failed to provide consumers with adverse action notices as required by the FCRA. Section 615(a) of the FCRA requires consumers to receive an adverse action notice whenever information in a consumer report is used (in whole or in part) to make a decision adverse to the consumer, such as the denial of a loan application. The adverse action notice alerts the consumer to the fact that information in a consumer report has factored in the decision-making process and provides the consumer with the opportunity to access the consumer report and address any errors.

Outcome: Quicken Loans entered into a consent decree with the FTC, agreeing to provide consumers with notices that comply with the FCRA whenever it takes adverse actions against them. The FTC allowed Quicken Loans to restructure its online application process to allow it to avoid triggering the adverse action notice requirement: "Under the proposed order, the FTC would not view Quicken Loans' failure to grant an online request for preapproval as an adverse action if the company meets certain specific requirements, including that:

- Quicken Loans provides a clear and conspicuous disclosure in close proximity to the preapproval offer that preapproval may be granted online or offline; and

- if Quicken Loans determines it cannot grant preapproval online because it needs additional information, it notifies the consumer that: 1) the request for preapproval has not been denied, but that Quicken Loans needs additional information from the consumer; and 2) if the consumer submits the additional information, Quicken Loans will decide whether to grant the request and inform the consumer of its decision.

Fine Imposed: None

In 2003, the FCRA was amended by The Fair and Accurate Credit Transaction Act ("FACTA"), which added substantive new provisions to the FCRA to address identity theft and to improve the accuracy of consumer reports. For example, to help combat identity theft, FACTA revised the FCRA to provide for new classes of fraud alerts that consumers could add to their credit reports.

Because consumer reports contain Social Security numbers and other sensitive personal information, FACTA also revised the FCRA to require users of consumer reports to securely dispose of them. Pursuant to this amendment, the Federal Trade Commission has published a Disposal Rule, which sets the standards that companies using consumer reports must follow when disposing of any paper or media containing consumer reporting information. As discussed in Chapter 4, the Federal Trade Commission, like most regulators, aggressively enforces when companies fail to take appropriate measures to secure sensitive personal information.
THE AMERICAN UNITED MORTGAGE CASE (DECEMBER 2007)

Respondent: American United Mortgage Company

Regulator: Federal Trade Commission

Basis for Complaint: Violation of Fair Credit Reporting Act (Disposal Rule) as well as violations of the Gramm-Leach-Bliley Act Safeguards Rule and Privacy Rule

Facts and Allegations: American United Mortgage collects sensitive personal information from and about consumers, including credit reports and sensitive financial information. The FTC complaint alleged that the company failed to implement reasonable policies and procedures to protect the sensitive information, as required by the GLBA Safeguards Rule, and failed to properly dispose of consumer reports, as required by the FCRA Disposal Rule. The complaint also alleged that the company failed to otherwise comply with the GLBA Privacy Rule, by not providing required consumer privacy notices.

As a result of the Safeguards Rule and Disposal Rule violations, the FTC noted that hundreds of documents containing sensitive personal information were tossed into an unsecured, easily accessible public dumpster, including 36 consumer reports.

Outcome: The settlement with the FTC requires American United Mortgage to:

(1) Comply fully with the Disposal Rule, Safeguards Rule and Privacy Rule;

(2) Obtain, every two years, for the next ten years, an audit performed by a qualified, independent third party professional to ensure that its security program meets the requirements of the order; and

(3) Pay a civil money penalty.

Fine Imposed: $50,000 for violation of the FCRA Disposal Rule

Finally, like most data protection laws, the Fair Credit Reporting Act requires entities to maintain reasonably accurate information about consumers. The Act prohibits reporting obsolete information, and requires furnishers of information to consumer reporting agencies to address any accuracy issues.

In August 2000, the Federal Trade Commission announced a settlement with Performance Capital Management (“PCM”). The Federal Trade Commission had accused PCM of routinely reporting inaccurate information to consumer reporting agencies and refusing to investigate consumer disputes. (PCM purportedly reported incorrect delinquency dates for consumer accounts, resulting in negative information appearing incorrectly on consumer reports.) In settling the charges, PCM was enjoined from committing any further violations of the FCRA’s accuracy provision and assessed a $2,000,000 penalty.xxvii

Healthcare Information and Medical Records

The Health Insurance Portability and Accountability Act of 1998 (“HIPAA”) directed the U.S. Department of Health and Human Services (“HHS”) to promulgate privacy and security rules to govern the handling of personal information by healthcare providers, health insurance companies and healthcare clearinghouses. HHS has the authority to enforce these rules. The HHS Office of Civil Rights (“OCR”) enforces
the HIPAA Privacy Rule, while the HHS Centers for Medicare and Medicaid Services ("CMS") enforces the 
HIPAA Security Rule.

Although there have not yet been many high-profile HIPAA actions, both OCR and CMS have been working 
with companies covered by the HIPAA rules to address non-compliance.

THE HIPAA PRIVACY RULES CASE

Respondent(s): Various companies – see details below

Regulator: Department of Health and Human Services, Office of Civil Rights

Basis for Complaint: Violations of the HIPAA Privacy Rule

Facts, Allegations and Outcomes: The following case summaries are posted on the OCR 
website. These reflect a sample of the OCR enforcement activities around the Privacy Rule.xxviii

(1) Inappropriate Disclosures of Protected Health Information

- **Large Provider Revises Process to Prevent Unauthorized Disclosures to Employers**
  A state health sciences center disclosed protected health information to a complainant's 
  employer without authorization. Among other corrective actions to resolve the specific issues in 
  the case, including mitigation of harm to the complainant, OCR required the Center to revise its 
  procedures regarding patient authorization prior to release of protected health information to an 
  employer. All staff was trained on the revised procedures.

- **Public Hospital Corrects Impermissible Disclosure of Protected Health Information in 
  Response to a Subpoena**
  A public hospital, in response to a subpoena (not accompanied by a court order), impermissibly 
  disclosed the protected health information (PHI) of one of its patients. Contrary to the Privacy 
  Rule protections for information sought for administrative or judicial proceedings, the hospital 
  failed to determine that reasonable efforts had been made to insure that the individual whose 
  PHI was being sought received notice of the request and/or failed to receive satisfactory 
  assurance that the party seeking the information made reasonable efforts to secure a qualified 
  protective order. Among other corrective actions to remedy this situation, OCR required that 
  the hospital revise its subpoena processing procedures. Under the revised process, if a 
  subpoena is received that does not meet the requirements of the Privacy Rule, the information 
  is not disclosed; instead, the hospital contacts the party seeking the subpoena and the 
  requirements of the Privacy Rule are explained. The hospital also trained relevant staff 
  members on the new procedures.

- **Outpatient Surgical Facility Corrects Privacy Procedure in Research Recruitment**
  An outpatient surgical facility disclosed a patient’s protected health information (PHI) to a 
  research entity for recruitment purposes without the patient's authorization or an Institutional 
  Review Board (IRB) or privacy-board-approved waiver of authorization. The outpatient facility 
  reportedly believed that such disclosures were permitted by the Privacy Rule. OCR provided 
  technical assistance to the covered entity regarding the requirement that covered entities 
  seeking to disclose PHI for research recruitment purposes must obtain either a valid patient 
  authorization or an Institutional Review Board (IRB) or privacy-board-approved alteration to or
waiver of authorization. Among other corrective actions to resolve the specific issues in the case, OCR required the outpatient facility to: revise its written policies and procedures regarding disclosures of PHI for research recruitment purposes to require valid written authorizations; retrain its entire staff on the new policies and procedures; log the disclosure of the patient's PHI for accounting purposes; and send the patient a letter apologizing for the impermissible disclosure.

(2) Safeguarding Protected Health Information

• **Pharmacy Chain Institutes New Safeguards for Protected Health Information**
  A grocery store based pharmacy chain maintained pseudoephedrine log books containing protected health information in a manner so that individual protected health information was visible to the public at the pharmacy counter. Initially, the pharmacy chain refused to acknowledge that the log books contained protected health information. OCR issued a written analysis and a demand for compliance. Among other corrective actions to resolve the specific issues in the case, OCR required that the pharmacy chain implement national policies and procedures to safeguard the log books. Moreover, the entity was required to train all of its staff on the revised policy. The chain acknowledged that log books contained protected health information and implemented the required changes.

• **Large Medicaid Plan Corrects Vulnerability that Had Resulted in Wrongful Disclosure**
  A municipal social service agency disclosed protected health information while processing Medicaid applications by sending consolidated data to computer vendors that were not business associates. Among other corrective actions to resolve the specific issues in the case, OCR required that the social service agency develop procedures for properly disclosing protected health information only to its valid business associates and to train its staff on the new processes. The new procedures were instituted in Medicaid offices and independent health care programs under the jurisdiction of the municipal social service agency.

• **Health Plan Corrects Computer Flaw that Caused Mailing of EOBs to Wrong Persons**
  A national health maintenance organization sent explanation of benefits (EOB) by mail to a complainant's unauthorized family member. OCR's investigation determined that a flaw in the health plan's computer system put the protected health information of approximately 2,000 families at risk of disclosure in violation of the Rule. Among the corrective actions required to resolve this case, OCR required the insurer to correct the flaw in its computer system, review all transactions for a six month period and correct all corrupted patient information.

(3) Respecting Rights of Access

• **Private Practice Revises Process to Provide Access to Records**
  A private practice failed to honor an individual's request for a complete copy of her minor son's medical record. OCR's investigation determined that the private practice had relied on state regulations that permit a covered entity to provide a summary of the record. OCR provided technical assistance to the covered entity, explaining that the Privacy Rule permits a covered entity to provide a summary of patient records rather than the full record only if the requesting individual agrees in advance to such a summary or explanation. Among other corrective actions to resolve the specific issues in the case, OCR required the covered entity to revise its policy. In addition, the covered entity forwarded the complainant a complete copy of the medical record.

• **Private Practice Revises Process to Provide Access to Records**
  At the direction of an insurance company that had requested an independent medical exam of
an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.

With regard to the HIPAA Security Rule, the CMS has enforcement authority. CMS’ published December 2007 enforcement statistics report indicates that it has considered 379 Security Rule complaints, of which 99 are still open and 280 have been resolved. Of the resolved cases, CMS reports that 49 of the cases (17.5%) were closed after corrective action was taken.xxix

Medical records, of course, contain some of the most sensitive types of data that exist. Outside the United States, medical information is also classified as sensitive or, in European parlance, one of the “special categories of data.” Companies are generally expected to obtain consent for the processing of sensitive data. In some jurisdictions, such as Dubai International Financial Centre, a special permit must be obtained from the data protection authority before sensitive data can be processed.
Companies may also face contractual claims, but these are typically brought by private parties. This Case Book focuses on actions brought against companies by regulators; private litigation for privacy and security claims is outside the scope of this work.

FTC website: http://www.ftc.gov. Cases presented can be found by following “enforcement links” in the various sections devoted to laws enforced by the FTC.

Federal Communications Commission website: http://www.fcc.gov/


For a general discussion, see: http://www.naag.org/what_does_an_attorney_general_do.php; see also state AG websites, such as: http://ag.ca.gov/ (CA), http://www.oag.state.ny.us/home.html (NY), and http://www.oag.state.tx.us/ (TX)

A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (Revised September 2002) online at http://www.ftc.gov/ogc/brfovrvw.shtm


See list of FTC cases: http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf.html

A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (Revised September 2002) online at http://www.ftc.gov/ogc/brfovrvw.shtm

See, e.g., 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule


The CAN SPAM Act of 2003 has limited preemption.

16 C.F.R. pt. 310

FTC’s Facts for Business: Complying with the Telemarketing Sales Rules (January 2004)

FTC Press Release: FTC Announces Law Enforcement Crackdown on Do Not Call Violators: Six Settlements Require Payment of Nearly $7.7 Million in Civil Penalties; Additional Complaint Charges Telemarketer with Multiple DNC-Related Violations (November 7, 2007)

See http://ago.mo.gov/ for information on the Missouri No-Call Registry

Nixon fines telemarketer $15,000 for violating No Call law. Branson Daily News (Branson, Missouri), January 15, 2008

Calif. Bus. & Prof. Code § 17538.43

The primary purpose of an email is determined by what a reasonable recipient would perceive the purpose of the message to be based upon its subject line and the content located at the beginning of the message. CAN SPAM Act “Primary Purpose” Final Rule (2004).

See the discussion of the Children’s Online Privacy Protection Act (COPPA) in Chapter 7. The Xanga case summary illustrates the application of COPPA to social networking sites in the United States.


See FTC Guidance on the Children’s Online Privacy Protection Act, online at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html

FTC File No.: 982-3542, In the matter of Performance Capital Management, Inc. Please note that the $2,000,000 fine was suspended due to the financial condition of PCM.

http://www.hhs.gov/ocr/privacy/enforcement/casebyentity.html