Privacy Law 2009: A Year of Change

Ann E. Tobin, UnitedHealth Group Incorporated
Senior Privacy Counsel

Ross C. D’Emanuele, Dorsey & Whitney LLP
(612) 343-2161
d.emanuele.ross@dorsey.com

Barry D. Glazer, Dorsey & Whitney LLP
44 (0)20 7826 4508
glazer.barry@dorsey.com

Melissa J. Krasnow, Dorsey & Whitney LLP
(612) 492-6106
krasnow.melissa@dorsey.com

William R. Stoeri, Dorsey & Whitney LLP
(612) 343-7942
stoeri.bill@dorsey.com

Contents

1. PowerPoint

2. Frequently Asked Questions Relating to Transfers of Personal Data from the EUZEA to Third Countries, published by EU Commission


Privacy Law 2009: A Year of Change

Ann E. Tobin
Senior Privacy Counsel, UnitedHealth Group Incorporated

Ross C. D’Emanuele, Barry D. Glazer, Melissa J. Krasnow and William R. Stoeri
Dorsey & Whitney LLP
## Privacy Laws

### State

- Data breach notification
- Payment card
- Encryption (Nevada)
- Security procedures
- Document destruction
- Social Security number
- Encryption (Massachusetts)

### Federal

- Federal Trade Commission
  - Cases
  - Guidance
- Red Flags Rule
- Notice of Address Discrepancy Regulation
- Fair and Accurate Credit Transactions Act Disposal Rule
- Health Insurance Portability and Accountability Act
- Health Information Technology for Economic Clinical Health Act
- New York Stock Exchange Rule

### International

- European Union Data Protection Directive
- Other European Union Laws
The American Recovery and Reinvestment Act of 2009

- Signed into law February 17, 2009
- Title XIII, Subtitle D (HITECH ACT) significantly expands HIPAA Privacy and Security Law
  - Business Associates
  - Breach Notification
  - Penalties/Enforcement
What is a Business Associate?

- Anyone who, on behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information; or

- Provides legal, actuarial, accounting, consulting, management, administrative, accreditation or financial services for the covered entity that involve the disclosure of individually identifiable health information from the covered entity to the person.

45 C.F.R. Section 160.103
HIPAA Security Rules Now Directly Applicable to Business Associates

- Previously, BAs were subject only to the BA Agreement
- ARRA makes BAs subject to direct HIPAA Security regulation by HHS
Security Rules

- Administrative Safeguards – 45 C.F.R. Section 164.308
- Physical Safeguards – 45 C.F.R. Section 164.310
- Technical Safeguards – 45 C.F.R. Section 164.312
- Policies and Procedures and Documentation Requirements – 45 C.F.R. Section 164.316

Compliance Date: February 17, 2010
Breach Notification

Notification must occur upon discovery of a breach of “unsecured” protected health information

Breach occurs if there is “significant risk of harm”

Form and Content of Notice Mandated

May Require Media Notice

Notice to HHS immediately if more than 500 individuals affected; otherwise annual log submitted

74 Fed. Reg. 42740 (August 24, 2009)
Penalties/Enforcement:

- New Tiered Penalties with Potential for $50K per Violation with no Ceiling
- State AGs Can Enforce
- Audit Authority
- Whistleblower Rules
- HHS **Must** Impose Penalties if Willful Neglect
- Personal Liability?

13409 – 13411 of HITECH Act
DATA PROTECTION IN THE EU:
CONFLICT OR CONVERGENCE WITH US LAW?

Barry D. Glazer
Dorsey & Whitney LLP
London
DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

A. Background

1. The first data protection laws in Europe date from the 1970’s in Germany and France.

2. In contrast to the United States, the EU approach has been to enact a broad directive governing the protection of personal data rather than industry or sector specific legislation.

3. The EU Privacy Directive (1995/46/EC) enacted in 1995 is the basis for data protection laws implemented in each of the 27 EU member countries.


5. The EU data privacy concepts have on occasion presented challenging conflicts with US law. Recently, however, evolving privacy law in the US has served as a guide to the further expansion of data protection within the EU.
B. The EU Privacy Directive – Scope and Jurisdiction

1. The Directive applies only to “Personal Data”
   a) defined as any information relating to an identified or identifiable natural person. Data is identifiable personal data when it allows a person’s identity behind the data to be recovered directly or indirectly;
   b) excludes corporate data and anonymous data.

2. The Directive covers “Processing of Personal Data”, which includes any operation performed upon personal data, including manual and automatic collection, recording, storage, retrieval, use, disclosure and transmission of personal data.

3. The Directive applies to the processing of Personal Data by a Data Controller (the person who determines the purpose and use of the data processing) or a Data Processor (the person executing the processing for a data controller).
B. The EU Privacy Directive – Scope and Jurisdiction (cont’d)

4. The Directive raises complex issues of jurisdiction. As between the data protection laws of the various EU member countries, the country where the processing is carried out and the data controller is established applies. If a data controller is not established in any EU country, the EU privacy laws apply if the processing of personal data makes use of equipment situated within a EU member country unless the equipment is used only for purposes of transit through the country.
C. The Overall Principles of the EU Data Protection Laws

1. Personal Data must be processed fairly and lawfully;
2. Personal Data must be collected for specific and legitimate purposes;
3. Processing of Personal Data must be relevant and not in excess of the purposes for which the data was collected;
4. The Personal Data must be accurate and where necessary kept up to date; and
5. Personal Data must be kept in identifiable form only as long as necessary for the purposes for which the Personal Data was collected.
D. Principal Obligations imposed on a Data Controller under EU Law

1. Processing of Personal Data can only take place if:
   a) the Data Subject has given his unambiguous and explicit consent; or
   b) the processing of the Personal Data is necessary for the performance of a contract to which the data subject is a party; or
   c) processing meets certain other exemptions allowed by the law.
D. Principal Obligations imposed on a Data Controller under EU Law (cont’d)

2. Sensitive Personal Data is given special treatment and generally may not be processed without the Data Subject’s explicit consent. Sensitive Personnel Data includes social or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health or sex life. Certain exemptions apply, particularly where processing is required to deliver health care services.
D. Principal Obligations imposed on a Data Controller under EU Law (cont’d)

3. The Data Subject must be provided with information when the his personal data is collected, including:
   
a) the identity of the Data Controller;
   b) the intended purposes of the data processing;
   c) any further information necessary to guarantee fair processing, such as the identity of the recipients of the data, whether or not responses to questions are obligatory and the existence of the right of access and correction of the data concerning the data subject.

4. After collection, upon inquiry from the Data Subject, the Data Controller must provide the Data Subject with confirmation that data relating to him is being processed and grant the right to access and correct any inaccurate data.
D. Principal Obligations imposed on a Data Controller under EU Law (cont’d)

5. The Data Controller must take measures to ensure an appropriate level of security for the Personal Data taking into account the level of risks and nature of the data;

6. If the Data Controller confers processing of the data to a third party, the Data Controller must enter into a binding contract with the Data Processor to assure that the Data Processor only acts on instructions of the Data Controller and adheres to the same security obligations.

7. The Data Controller must notify the appropriate national Data Protection Authority (DPA) prior to commencing data processing operations (subject to various exemptions allowed under national law); and

8. Personal Data cannot be transferred to countries outside the EU unless the third country provides an “adequate level of protection” for Personal Data (subject to certain derogations discussed below).
E. Transfers of Personal Data Outside the EU – Conflict Resolved?

1. The prohibition in the EU Directive against transfers of Personal Data to countries not according an “adequate” measure of protection to Personal Data has presented problems for US based multinational companies.

2. The EU has only certified a limited number of countries it considers to have an adequate level of protection (currently Argentina, Canada, Guernsey, Isle of Man and Switzerland). Because the US does not have a general comprehensive data privacy law, the US is not on the approved list.
E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont’d)

3. Regardless of the country outside the EU to which the Personal Data is to be transferred, the transfer can legally take place if:

   a) the Data Subject has given his unambiguous consent to the transfer;

   b) the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller;

   c) the transfer is necessary for the conclusion or performance of a contract between the Data Controller and a third party concluded “in the interest of the Data Subject”;

   d) the transfer is necessary or required for the establishment, exercise or defense of legal claims; or

   e) the transfer is necessary to protect the vital interests of the Data Subject.
E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont’d)

4. The above exceptions often are problematic. For example, obtaining the consent of all Data Subjects may be impractical in a commercial context. In the case of a US parent’s foreign affiliates’ employees, some employees may refuse to consent to the transfer of their Personal Data to the US. Additionally, the validity of an employee’s consent is not uniformly accepted in all EU countries because of concerns about coercion.

5. Other means of legally transferring EU Personal Data to the US have been approved by the EU:

   a) Standard Data Export Contracts (the original form of standard contract approved by the EU for transfer of data from controller to controller or from controller to processor or the ICC alternative model contracts for transfers between controllers).
DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont’d)

i. The Data Controller remains liable to the Data Subject for breaches of security under all of the approved contracts forms; under the original standard contracts the data importer and data exporter have joint liability;

ii. The contract is normally bilateral and therefore cannot cover a number of data exporters in different EU countries;

iii. The contracts are subject to prior notice and/or approval requirements in a number of EU countries (e.g. France and the Netherlands); and

iv. Courts of the EU country where the data exporter is located retain jurisdiction over the parties, including claims by Data Subjects who are third party beneficiaries.
DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont’d)

b) US Safe Harbor

i. Provides self-certification of the US data importer that it provides for adequate protection to the specific type of Personal Data listed in the certification;

ii. Enforcement remains in the US through the FTC (or the Department of Transport if applicable);

iii. Is not available for use by financial institutions, telecommunication carriers or non-profit organizations;

iv. Requires adherence to the Safe Harbor Principles, which essentially mirror the EU Data Protection Principles;

v. Requires annual self-certification, periodic auditing of compliance and the establishment of a dispute mechanism for resolution of disputes brought by Data Subjects.
DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont’d)

c) Binding Corporate Rules (BCR)

i. First proposed in 2003, the BCR exemption from the cross-border prohibition on Personal Data transfers is a specifically structured internal code of conduct intended to allow a multinational group of companies to transfer Personal Data intra-group to affiliates anywhere within the world while assuring the security of the data and the rights of the Data Subjects.

ii. The BCR are subject to the initial authorization of the national data protection supervisory authority in one of EU member countries. Determination of which country’s supervisory authority is the “lead authority” is based on a number of factors, including where the group has its European headquarters, where an affiliate with delegated responsibility for data protection matters is located, where the most transfers out of the EU take place and the group affiliate within the EU best placed to enforce the BCR.
DATA PROTECTION IN THE EU: CONFLICT OR CONVERGENCE WITH US LAW?

E. Transfers of Personal Data Outside the EU – Conflict Resolved? (cont’d)

iii. The application for approval of the BCR must contain extensive information on the binding nature of the BCR within and outside the group, including details of a data protection audit plan, the security safeguards to be put into place for the personal data, description of the training program to be instituted, the processing and flow of information and the mechanism for reporting and complaints.

iv. Despite the submission of the application to the lead authority in one EU country, the other EU countries from which personal data will be exported must approve the BCR. Partly as a result of this cumbersome requirement in the past very few multinational companies have sought approval for data transfers on the basis of the BCR exemption.

v. The BCR must contain a duty for the EU headquarters or the delegated EU affiliate to accept responsibility for and remedy acts of members of the group outside the EU and to pay compensation for any damages resulting from violation of the BCR by group members. Any data subject has the right to bring an action for damages in EU courts for acts in violation of the BCR occurring outside the EU. The burden of proof lies with the company and not the individual Data Subject.
F. Recent Developments in EU Data Protection Law

1. Binding Corporate Rules

   a) The requirements for the BCR procedure for intra-group Personal Data transfers have been clarified by the issuance of a standard form checklist for the content of a BCR as well as the application form for the lead authority approval.

   b) A mutual recognition procedure has been established whereby the approval of the lead authority in one EU country will satisfy the approval requirement for all other EU countries that have agreed to the procedure, rather than having to obtain the separate approval of each EU country from which data will be exported. At present, 18 of the 27 EU countries have subscribed to the mutual recognition procedure.

   c) As a result of these recent changes, the BCR procedure is likely to be viewed more seriously by multinational companies as a realistic legal means of transferring Personal Data among group affiliates outside the EU.
F. Recent Developments in EU Data Protection Law (cont’d)

2. Data Breach Notification Requirements – Convergence with US law?

a) Although the EU Privacy Directive requires that Data Controllers must implement “appropriate technical and organizational measures” to protect personal data against accidental or unauthorized loss, destruction or disclosure, neither the Directive nor most of the national implementing laws impose a specific duty to notify either the national data protection authority or the Data Subject in the case of a data breach.

b) A number of highly public data breaches within the EU in recent years as well as the increasing regulation of data breaches in the US have brought demands for increasing the obligations of a Data Controller in the event of a data breach in the EU.

c) The EU has proposed imposing a mandatory notification requirements on public electronic communication service providers (essentially telecommunication and internet service providers) for data breaches, but there are increasing calls for a general US style data breach notification requirement to be added to the EU data privacy laws.
F. Recent Developments in EU Data Protection Law (continued)

d) Data breaches are to some extent covered in certain sectors at the national level. For example, financial companies in the UK regulated by the Financial Services Authority (FSA) are subject to fines for lax security procedures and controls. In a recent case, a national savings and loan company was fined nearly £1 million as a result of its mishandling of a laptop computer containing sensitive customer data stolen from an employee’s home.

3. Sarbanes-Oxley (SOX) Whistleblowing Compliance Schemes – Conflict with EU Privacy Laws?

a) The SOX requirement for the establishment of a hotline for communicating employee complaints has raised difficult issues under European laws.

b) One of the most significant conflicts with US law relates to the perceived conflict between the requirement imposed by SOX for the availability of submitting whistleblowing complaints anonymously and the protection of individual employees’ labor and data privacy rights.
F. Recent Developments in EU Data Protection Law (cont’d)

c) Several EU countries, most notably France, the Netherlands and Germany as well as the EU Committee of national data privacy supervisors, have issued guidance notes designed to define the extent to which whistleblowing hotlines can be implemented consistent with EU data privacy concepts. The guidance notes render the hotline less effective.

4. Employer monitoring of employee e-mails

a) While common in the US, monitoring of employee e-mails in the EU presents data privacy issues in a number of countries, including potential criminal penalties.

b) The regulatory interpretation of the employer’s right to monitor versus the employee’s expectation of privacy of communications varies considerably among EU countries.
II. Step-by-step decision-making process

The following process should be undertaken before any transfer of personal data takes place:

**STEP 1**

The first question to ask is whether the data being exported include any personal data.

- **NO**
  - If the data to be transferred are not considered to be personal data then the transfers may take place.

- **YES**
  - If the data are personal data, the second question to ask is whether, prior to the transfer, the data have been collected and further processed in accordance with the national law applicable to the processing activity. For more details, see here.

- **NO**
- **YES**
  - If, prior to the transfer, the personal data have not been lawfully collected or further processed, in accordance with the national law applicable, the processing is not lawful and should not be carried out. As a result the transfer may not take place.
  - Is the purpose of the transfer compatible with the one for which the data were initially collected and processed, in accordance with the national law applicable to the processing activity? For more details, see here.

- **NO**
- **YES**
  - If the purpose of the transfer is incompatible with the one for which the data were initially collected, then the transfer may not take place, in principle, unless it is legally required by national legislation applicable to the processing activity.
  - If, before and during the transfer, the personal data have been lawfully collected and further processed, in accordance with the national law applicable, then proceed to **STEP 2**.
**STEP 2**

Will the data be transferred to a country or territory within the European Union or the European Economic Area?

- **YES**
  - If the data are transferred to a EU or EEA country, then the transfer may proceed.

- **NO**
  - Is the data transferred to a third country considered as offering an adequate level of protection?
    - See the List of countries considered adequate.
      - **YES**
        - If the data are transferred to a country considered as offering an adequate level of protection, or if it is covered by the Safe Harbor commitments of a US company that has signed up to the Safe Harbor scheme, the transfer may take place.
        - See the Safe Harbor list.
      - **NO**
        - The data are transferred to a third country that does not provide an adequate level of protection (or to a US company that has not joined the Safe Harbor scheme). Proceed to STEP 3.

For more details on this step, please refer to the FAQs on general questions.
STEP 3

Are the data transferred to a recipient in a third country that does not provide an adequate level of protection?

GO BACK TO STEP 2.

YES

Are the data transferred between companies belonging to the same multinational corporation?

PROCEED TO STEP 4.

NO

Is the controller responsible for the transfer putting in place adequate safeguards and has the national data protection authority approved the transfer?

To provide adequate safeguards for their transfers, data controllers can consider using standard contractual clauses.

The Commission has approved three types of standard contractual clauses to facilitate the implementation of this solution.

NO

The transfer may not take place unless one of the exceptions laid down in Article 26(1) can be relied on.

NO

YES

See the FAQs on standard contractual clauses.

See the FAQs on the Article 26(1) derogations.
STEP 4

Are the data transferred between companies belonging to the same multinational corporation established in third countries that do not ensure an adequate level of protection?

NO

Go back to STEP 2.

YES

Has the multinational corporation adopted binding corporate rules that are approved by the national data protection authority?

YES

See the FAQs on binding corporate rules.

OR ALTERNATIVELY

Do the companies use standard contractual clauses for transfers of personal data between companies belonging to the same multinational corporation?

YES

See the FAQs on standard contractual clauses.

NO

If the use of standard contractual clauses or binding corporate rules is not practical and/or feasible, the transfer may not proceed unless one of the exceptions laid down in Article 26(1) can be relied on.

See the FAQs on the Article 26(1) derogations.
Where Privacy and Corporate Governance Laws Meet

Information Security Obligations

By Melissa J. Krasnow

[Editor's Note: This is the first in a series of articles addressing some of the key issues surrounding corporate responsibility with respect to the privacy of information and security breaches.]

As business information, particularly in electronic format, continues to proliferate, the need to maintain the security of this information is increasing. There are privacy and corporate governance laws that govern the obligation of a company to keep information secure. According to the Global State of Information Security 2006, a worldwide study by CIO magazine, CSO magazine and PricewaterhouseCoopers representing the responses of almost 7800 senior executives, “Noncompliance runs broad and deep in all industries, and ignorance of applicable law is a big factor.” This article provides an overview of two important information security obligations — security procedures and practices and document destruction — under privacy and corporate governance laws.

Security Procedures and Practices

State Security Procedures and Practices Laws

A few states have enacted laws regarding a company’s duty to maintain reasonable security procedures and practices. Arkansas, California, Nevada, Rhode Island, and Texas and Utah enacted security procedures and practices laws. California was the first state to enact a security procedures law. Under the California law, a company that owns or licenses personal information about a California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

Personal information means an individual’s first name or first initial and last name in combination with any of the following data elements, when either the name or data elements are not encrypted: 1) Social Security number, 2) driver’s license number or state identification card number, 3) account number, credit card number or debit card number in combination with any required security code, access code or password (e.g., a PIN) that would permit access to an individual’s financial account or (iv) medical information.

Federal Trade Commission Security Procedures Standards

Although there is no specific federal security procedures law for all companies, the Federal Trade Commission has described standards for security procedures in a number of recent cases. By way of example, in the BJ’s Wholesale Club case in 2005, the FTC charged that BJ’s failure to provide reasonable security for sensitive customer information was an unfair act or practice in violation of Section 5 of the Federal Trade Commission Act because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. The FTC alleged that BJ’s: 1) failed to encrypt consumer information when it was transmitted or stored; 2) stored the information longer than it had a need to do so; 3) stored the information in files that could be accessed using commonly known default user IDs and passwords; 4) failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and 5) failed to use measures sufficient to detect unauthorized access to the networks. The settlement order for this case requires BJ’s to establish and maintain a comprehensive information security program that includes administrative, technical and physical safeguards and to obtain regular third party professional audits of this program for compliance with the FTC Order and with book-keeping and record-keeping requirements. The FTC Order is in effect for a 20-year period.

Sarbanes-Oxley Act

Pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 (SOX), management of a public company is responsible for establishing and maintaining adequate internal control over its financial reporting. Management must evaluate and report on the effectiveness of internal control over financial reporting in the annual report filed by a public company with the Securities and Exchange Commission. This management report is accompanied by an attestation from the independent auditor of the public company. Management also must evaluate and disclose changes that have materially affected or are reasonably likely to materially affect a public company’s internal control over financial reporting in the quarterly and annual reports. Moreover, the Chief Executive Officer and Chief Financial Officer of a public company must provide certifications regarding their responsibility for establishing and maintaining internal control over financial reporting and the design of internal control over financial reporting to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. These certifications are attached as exhibits to a public company’s quarterly and annual reports.

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP (e-mail: krasnow.melissa@dorsey.com).
In re Caremark

This suit against the board of directors of Caremark International Inc. involved claims that the directors breached their fiduciary duty of care to the company in connection with alleged violations by Caremark employees of state and federal laws. In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del.Ch. 1996). The plaintiffs sought to recover losses on behalf of the company from the directors. According to the Delaware Chancery Court:

[It is important that the board exercise a good faith judgment that the corporation’s information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility . . . [A] director’s obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.

**Document Destruction**

**State Document Destruction Laws**

Close to one-third of states have enacted laws requiring the destruction of documents. Arkansas, California, Hawaii, Indiana, Kansas, Kentucky, Montana, Nevada, New Jersey, North Carolina, Rhode Island, Tennessee, Texas, Utah, Vermont and Washington enacted document destruction laws. Under the California law, a company must take all reasonable steps to destroy or arrange for the destruction of the records of a customer within its custody or control containing personal information which is no longer to be retained by: 1) shredding, 2) erasing, or 3) otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means.

Personal information means any information that identifies, relates to, describes or is capable of being associated with, a particular individual, including: 1) name; 2) signature; 3) Social Security number; 4) physical characteristics or description; 5) address; 6) telephone number; 7) passport number; 8) driver’s license or state identification card number; 9) insurance policy number; 10) education; 11) employment; 12) employment history; 13) bank account number; 14) credit card number; 15) debit card number or 16) any other financial information. “Records” refers to any material regardless of the physical form on which information is recorded or preserved by any means (e.g., in written or spoken words, graphically depicted, printed or electromagnetically transmitted).

**Fair and Accurate Credit Transactions Act**

The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires a company that maintains or otherwise possesses consumer information for a business purpose to properly dispose of consumer information by taking reasonable measures to protect against unauthorized acquisition or use of the information in connection with its disposal. Consumer information means any record about an individual in paper, electronic or other form that is derived from a consumer report or a compilation of such record. Disposal refers to the discarding or abandonment of consumer information or the sale, donation or transfer of any medium (including computer equipment) upon which consumer information is stored.

Reasonable measures include establishing and complying with policies to: 1) burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed; 2) destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; and 3) conduct due diligence and hire a document destruction contractor or dispose of material specifically identified as consumer report information. Although the FACTA Disposal Rule applies to consumer reports and the information derived therefrom, the FTC, which enforces this Rule, encourages those that dispose of any records containing a consumer’s personal or financial information to take similar protective measures.

**SOX**

Two sections under SOX that cover document destruction apply to a company, whether public or private. Section 802 of the Sarbanes-Oxley Act states:

[W]hoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined … imprisoned not more than 20 years, or both.

Section 1102 of SOX states in pertinent part:

[W]hoever corruptly … alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object’s integrity or availability for use in an official proceeding; or … otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so … shall be fined … or imprisoned not more than 20 years, or both.

**Conclusion**

As information security obligations are continually changing, the laws governing information security obligations are evolving. Laws in different areas like privacy and corporate governance are both addressing these obligations. As a result, a company must carefully and constantly monitor developments in all of these laws in order to comply with them. According to the Ernst & Young 2006 Global Information Security Survey, compliance requirements in the past year have most significantly impacted and in the next year likely will continue to significantly impact the information security practices of companies.

Next month, the author will outline the requirements for providing notification of a security breach under state security breach notification law by any company and the factors that a public company needs to take into account regarding whether to disclose a security breach under federal securities law.
Disclosing Information Security Breaches Under Privacy and Securities Laws

By Melissa J. Krasnow

The Privacy Rights Clearinghouse estimates that over 100 million records containing sensitive personal information have been involved in security breaches. This non-profit consumer organization has tracked these breaches on its website (www.privacyrights.org) beginning with the significant and well-publicized ChoicePoint breach in February 2005. As a result, over two-thirds of states enacted security breach notification laws governing the notification that a company must make in the event of a security breach. This article outlines the requirements for providing notification of a security breach under state security breach notification law by any company and the factors that a public company needs to take into account regarding whether to disclose a security breach under federal securities law.

STATE SECURITY BREACH NOTIFICATION LAW

The following 34 states enacted security breach notification laws: Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington and Wisconsin. In addition, Michigan passed such a law with an effective date of July 2, 2007. It is important to note that Congress is considering federal security breach notification legislation and it is anticipated that a federal security breach notification law will be enacted in the coming years. But until a federal law is enacted that preempts the state notification breach laws, compliance with the various applicable state laws is required.

California was the first state to enact a security breach notification law. The California Security Breach Information Act (S.B. 1386) became effective July 1, 2003. Since the California law serves as a model for a number of the other state laws, this article discusses the California law. In practice, it is necessary to refer to all state laws that are applicable to a specific situation.

APPLICATION

The California law applies to a company that does business in California and owns or licenses computerized data that contains personal information. A company could be deemed to be doing business in California merely by maintaining personal information about a California resident. Also, a company could own or license computerized data containing personal information that is physically located outside of California but still be subject to the California law.

DEFINITION OF PERSONAL INFORMATION

Personal information means an individual’s first name or first initial and last name in combination with any of the following data elements, when either the name or data elements are not encrypted: 1) Social Security Number; 2) driver’s license number or state identification card number; or 3) account number, credit card number or debit card number in combination with any required security code, access code or password (e.g., a PIN) that would permit access to an individual’s financial account. But publicly available information that is lawfully made available to the general public from federal, state or local government records does not constitute personal information. It is important to note that this definition is substantially simi-
lar to the definition of personal information under the California security procedures law. The difference is that medical information is not included under the definition of personal information.

**DEFINITION OF SECURITY BREACH**

A security breach refers to the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the company. However, a good-faith acquisition of personal information by an employee or agent of the company for its purpose if the personal information is not used or subject to further unauthorized disclosure is not a security breach.

**NOTIFICATION OF SECURITY BREACH**

Following the discovery or notification of a security breach, the company must disclose the security breach to any California resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Moreover, a company that maintains computerized data that includes personal information that it does not own needs to notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. Notification must be made in the most expeditious manner consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Notification can be provided in any of the following ways: 1) written notice; 2) electronic notice in compliance with the provisions of the Electronic Signatures in Global and National Commerce Act (E-SIGN); or 3) substitute notice, if the company demonstrates that: (a) the cost of providing notice would exceed $250,000; (b) the affected class of subject persons to be notified exceeds 500,000; or (c) the entity does not have sufficient contact information. Substitute notice must consist of all of the following: 1) e-mail notice when the company has an e-mail address for the subject person or business; 2) conspicuous posting of the notice on the Web site of the business; and 3) notification to major statewide media.

Alternatively, a company that maintains its own notification procedures as part of an information security policy for the treatment of personal information and which is otherwise consistent with the timing requirements described above is compliant if it notifies subject persons in accordance with its policies in the event of a security breach.

**FEDERAL SECURITIES LAW**

A public company must consider whether to disclose a security breach in its reports with the Securities and Exchange Commission (SEC). While there is no specific obligation to disclose a security breach under federal securities law, there are reasons for doing so and there is precedent.

**SECURITIES EXCHANGE ACT OF 1934**

The disclosure controls and procedures of a public company must be designed to ensure that information required to be disclosed by the public company in its SEC reports under the Securities Exchange Act of 1934 (1934 Act) is accumulated and communicated to its management, including its Chief Executive Officer and its Chief Financial Officer, to allow for timely decisions regarding required disclosure. Disclosure controls and procedures means controls and other procedures that are designed to ensure that information required to be disclosed by the public company in its SEC reports is recorded, processed, summarized and reported within the requisite time periods.

A public company files periodic and current reports with the SEC to provide material information about the public company. Material information is information that a reasonable investor would consider important in making an investment decision. Additional considerations concerning the disclosure of a security breach include regulatory requirements and public relations.

A prominent example of the disclosure of a security breach in SEC reports is ChoicePoint, regarding the above-referenced breach that was made in a current report on Form 8-K under the heading for information that is not specifically required to be disclosed but that the public company deems to be of importance to security holders. ChoicePoint also disclosed in this current report that it was the subject of inquiries by various regulators, including the SEC, the Federal Trade Commission and state attorneys general. Subsequent disclosures about this matter were made by ChoicePoint in its periodic and current reports.

It is interesting to note that the SEC inquiry related to trading in ChoicePoint stock by the Chief Executive Officer and the Chief Operating Officer. The 1934 Act and the rules promulgated thereunder and the insider trading policy of a public company prohibit trading by officers and directors in the stock of a public company on the basis of material nonpublic information. A security breach before disclosure could constitute material nonpublic information.

**STOCK EXCHANGE RULES**

In addition to its SEC reporting considerations, a public company must take into account the stock exchange rules regarding the disclosure of material news (e.g., New York Stock Exchange and NASDAQ), if applicable.

**CONCLUSION**

Disclosures about security breaches are becoming more numerous resulting in part from the recent enactment of various state security breach notification laws. As more public companies suffer security breaches and are required to make these notifications, they will need to consider whether to make disclosures in their SEC reports and comply with federal securities law and any applicable stock exchange rules. Accordingly, a public company should make sure that its privacy and securities law compliance procedures and practices are consistent.
Enforcement Under State Security Breach Notification Laws

By Melissa J. Krasnow

Part Three of a Three Part Article

Thirty-four states — Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington and Wisconsin — have enacted security breach notification laws. And Michigan passed such a law with an effective date of July 2, 2007. These laws cover the notification that a company must make in the event of a breach of security of its system with respect to computerized personal information. How are these laws enforced in the event of a violation? These laws vary in terms of enforcement and penalties, as more particularly described below. This article provides an overview of the enforcement of these laws and describes examples of penalties.

**Enforcement by State Attorney General or State Regulator**

**State Attorney General Enforcement**

A number of laws provide for enforcement by the state attorney general. Some laws provide that the attorney general may bring an action for injunctive relief. Other laws provide that the attorney general may bring an action in law or equity to address violations and for other relief to ensure compliance or to recover direct economic damages resulting from a violation, or both. Certain of these laws specify civil penalty amounts. For example, the Texas attorney general may bring suit to recover a civil penalty of between $2000 to $50,000 for each violation of the law, may bring an action for injunctive relief and is entitled to recover reasonable expenses in obtaining injunctive relief, civil penalties, or both. The court also may grant other equitable relief. The New York attorney general may bring an action for injunctive relief, and the court may award damages for actual costs or losses, including consequential financial losses, incurred by a person entitled to notice under the state law where notification was not provided. The court also may impose a civil penalty of up to $150,000 for a knowing or reckless violation.

**State Regulator Enforcement**

Some laws provide for enforcement by the attorney general or a state regulator. By way of example, the Hawaii law provides for enforcement by the attorney general or the Hawaii Office of Consumer Protection. The Maine law provides for enforcement by the attorney general or the Maine Department of Professional and Financial Regulation, where applicable.

**Private Right of Action**

Some laws provide for a private right of action. For instance, the California and Washington laws provide that a violation of the state law constitutes a violation of that state’s unfair practice or similar law (e.g., Connecticut and Illinois).

**Examples of Penalties**

**Administrative Fines**

The Florida law provides for administrative fines. A person required to make a security breach notification that fails to do so within 45 days following the determination of a breach or receipt of notice from law enforcement is liable for an administrative fine in the amount of $,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period for up to 180 days. If no notification is made within the 180-day period, the person is subject to an administrative fine of up to $500,000. These fines apply per breach and not per individual affected by the breach. The Florida Department of Legal Affairs may bring proceedings to assess and collect these fines.

**Criminal Penalties**

The Minnesota law provides for criminal penalties.

**Corporate Dissolution or Revocation of Authority**

The Vermont law provides for the authority of the attorney general, a state’s attorney or a court to dissolve a domestic corporation or revoke the certificate of authority of a foreign corporation for a violation of the Vermont law.

**Violation of State Unfair Practice Law**

It is important to note that a number of state laws provide that a violation of the state law constitutes a violation of that state’s unfair practice or similar law (e.g., Connecticut and Illinois).

**Conclusion**

Given how these state laws vary in terms of enforcement and penalties, it is imperative to refer to the state laws that are applicable to a particular situation for guidance. Congress is considering federal security breach notification legislation. But the different state security breach notification laws will continue to apply until a federal law is enacted that preempts these laws.

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP, Minneapolis. She may be reached at krasnow.melissa@dorsey.com
Connecticut, Massachusetts and Nevada recently enacted laws requiring businesses to institute certain compliance measures to secure personal information that can be used to perpetrate identity theft. The Massachusetts law applies to a business located anywhere in the United States that stores or maintains personal information about a Massachusetts resident. This article discusses the requirements of these new state laws and their practical significance for businesses.

The personal information at issue includes Social Security, driver’s license and financial account numbers, each in combination with a person’s name. Forty-four states, including Connecticut, Massachusetts and Nevada, currently require businesses to notify individuals if there is a breach of personal information. This notification permits individuals to take steps to protect their credit cards and bank accounts from identity theft. Rather than simply requiring businesses to respond to a data breach with notifications, the new Connecticut, Massachusetts and Nevada laws impose certain compliance obligations on businesses to protect personal information from a data breach.

The Nevada and Connecticut laws each became effective on Oct. 1, 2008. The Nevada law, the least onerous of the three, mandates that “[a] business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.” Nev. Rev. Stat. § 597.970(1). Connecticut’s security measures go beyond encryption. Businesses must “safeguard the data, computer files and documents containing the information from misuse by third parties” and “destroy, erase or make unreadable such data, computer files and documents prior to disposal.” Conn. Pub. Act 08-16, § 1.

In particular, the Connecticut law focuses on Social Security numbers and requires businesses to “create a privacy protection policy which shall be published or publicly displayed...on an Internet web page” to “protect the confidentiality of...prohibit unlawful disclosure of...and limit access to Social Security numbers.” Conn. Pub. Act 08-167. There is a civil penalty of $500 for each intentional violation, up to a maximum of $500,000 “for any single event.” Id.

The Massachusetts regulation will require businesses storing residents’ information to set up data compliance programs.

Massachusetts’ regulation is the most comprehensive

A first-of-its-kind Massachusetts regulation issued by the state Office of Consumer Affairs and Business Regulation is the most comprehensive of the new laws. Businesses that own, license, store or maintain personal information about a Massachusetts resident must be in full compliance with this regulation on or before Jan. 1, 2010, including implementing a comprehensive, written information security program for personal information. 201 Mass. Code Regs. 201, 17.03-17.05. The Massachusetts attorney general is responsible for its enforcement.

This regulation in effect mandates businesses to establish a data compliance program that is consistent with the requirements of the Federal Sentencing

By Nick Akerman and Melissa J. Krasnow

Nick Akerman is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data. Melissa J. Krasnow is a partner in the firm’s Minneapolis office who focuses on privacy and security issues.
Guidelines. U.S. Sentencing Commission, Guidelines Manual, § 8B2.1 (November 2004). This regulation recognizes that the program must be tailored to each business based on the size, scope and type of business; the amount of resources available to the business; the amount of stored data maintained by the business; and the need for security and confidentiality of both consumer and employee information. 201 Mass. Code Regs. 17.03. Like the Federal Sentencing Guidelines, the program must address the following seven issues:

1. **Develop security policies.** Initially, businesses must identify the personal information they have and develop employee security policies that limit the amount of personal information collected and the time it is retained as well as restrict physical access to that information to those with a need to use it. These policies must also be enforced through technology that, at a minimum, secures user-authentication protocols; has secure access control measures; to the extent technically feasible, encrypts all transmitted records and files containing personal information that will travel across public networks, and all data to be transmitted wirelessly; has reasonable monitoring of systems for unauthorized use of, or access to, personal information; encrypts all personal information stored on laptops or other portable devices; has reasonably up-to-date firewalls and operating system security patches for files with personal information on a system connected to the Internet, reasonably designed to maintain the integrity of the information; and has reasonably up-to-date versions of system security agent software.

2. **Appoint a security coordinator.** One or more employees must be designated to manage the program.

3. **Minimize risk with third parties.** Care must be taken to ensure that those who might misuse personal information, such as terminated employees, do not have access to the data. Also, businesses must verify that third-party service providers with access to personal information have the capacity to protect this information in the manner provided for in this regulation and ensure that these service providers are applying security protective measures at least as stringent as those required to be applied to personal information under this regulation.

4. **Train the workforce.** Businesses must educate and train employees on the proper use of the computer security system and the importance of personal information security.

5. **Conduct regular audits.** At least annually, businesses must monitor the program and identify and assess risks to the security, confidentiality or integrity of records with personal information and evaluate the effectiveness of the current safeguards.

6. **Enforce the policies.** Businesses must impose disciplinary measures for violations and document responsive actions when a data security breach occurs.

7. **Respond to incidents.** Businesses must encourage employees to report violations and document responsive actions when a data security breach occurs.

These three new state laws augur what may be the start of a trend away from passive state regulation of personal information requiring a reactive approach when data are breached to stricter requirements aimed at protecting the data in the first instance. Previously, many states attempted to motivate businesses through their notification laws to encrypt or redact personal information to avoid the notification requirement in the event of a data breach. See, e.g., Kansas Stat. Ch. 50-7a01(h). In the future, more states are likely to require businesses to implement data security programs with varying degrees of complexity. Legislation is pending in Michigan and Washington to require businesses to encrypt stored personal data in accordance with accepted industry standards. A violation under the Michigan bill would be a misdemeanor with a 30-day maximum prison sentence and a $1,000 fine. Michigan Senate Bill No. 1022.

This trend toward proactive protection is evident in the federal system. Federal law requires financial institutions, 15 U.S.C. 6801 et seq., and health care providers, 42 U.S.C., 1320d et seq., to protect personal information. The Federal Trade Commission has responded to major data breaches by BJ’s Wholesale Club Inc. and DSW Inc. with enforcement actions requiring the establishment of comprehensive data security programs. By May 1, under the FTC’s “Red Flag” rules, financial institutions and creditors are required to conduct risk assessments and promulgate written programs designed to reduce and prevent identity theft. 16 C.F.R. pt. 681 appx. In the private sector, the New York Stock Exchange requires its listed companies to establish a data compliance program to protect “all non-public information that might be of use to competitors, or harmful to [a business] or its customers, if disclosed.” NYSE’s Listed Company Manual, § 303A.10.

## Adopting a comprehensive data compliance program

The message is clear. The way to ensure compliance with all of the existing and likely future state and federal regulation of personal data and to minimize the chance of being penalized is to adopt a comprehensive data compliance program. There are several obvious advantages to having such a program. First, it will help minimize costly data breaches. Often, one breach affects hundreds of thousands of individuals.

Second, if a suspected data breach does occur (since there is no foolproof means to prevent a data breach), a data compliance program provides the in-place mechanism and protocols to respond immediately to determine whether notifications have to be made to law enforcement or individuals and do whatever else is necessary to demonstrate to the authorities and the public that the business is acting responsibly.

Third, a data protection program for not much extra cost can include the protection of a business’ competitively sensitive data. Given the economic crisis and the increase in company downsizing, competitively valuable data is more vulnerable than ever to employee theft. There is a concern that “mass layoffs will incite a percentage of previously loyal employees to look at criminal activity” and “steal vital information” to start their own competing businesses or “to improve their job opportunities with the competition.” McAfee Inc., “Unsecured Economies: Protecting Vital Information,” February 2009 at 9-10, http://ciccentre.com/reports/Unsecured_Economies_012909.pdf.

Reprinted with permission from the March 9, 2009 edition of the NATIONAL LAW JOURNAL © 2009 Incisive Media US Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprintcustomerservice@incisivemedia.com. # 005-03-09-08
Changes Coming for Customer Personal Data

Is Your Company in Compliance?

By Melissa J. Krasnow

Nevada was the first state to enact a law requiring entities that transfer customer personal information outside of the secure system of the business through an electronic transmission (other than a facsimile) to use encryption. In late 2008, Massachusetts was the second state to pass legislation that mandates the use of encryption. Michigan is considering similar legislation. This is an area to watch as other states could consider such legislation.

The Massachusetts legislation goes beyond encryption, also requiring entities to develop, implement, maintain and monitor a comprehensive, written information security program on or before Jan. 1, 2010. This article describes the application of and the compliance requirements for the first-of-its kind Massachusetts regulation issued by the Massachusetts Office of Consumer Affairs and Business Regulation (“MOCABR”).

A Covered Entity must be in full compliance with this regulation on or before Jan. 1, 2010

Standards and Safeguards

This regulation establishes minimum standards to meet in connection with the safeguarding of personal information in paper and electronic records. The Program must be reasonably consistent with industry standards and contain administrative, technical and physical safeguards to ensure the security and confidentiality of these records. The safeguards in the Program must be consistent with the safeguards for protection of personal information and information of a similar character in any state or federal regulations to which the Covered Entity is subject. To determine whether the Program is compliant, the following factors must be considered: 1) the size, scope and type of business of the Covered Entity; 2) the amount of resources available to the Covered Entity; 3) the amount of stored data; and 4) the need for security and confidentiality of both consumer and employee information.

Requirements

The Program must do the following:

1. Designate one or more employees to maintain the Program;
2. Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality or integrity of any records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting these risks (e.g., ongoing temporary, contract and regular employee training, employee compliance with policies and procedures and means for detecting and preventing security system failures);
3. Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises;
4. Impose disciplinary measures for violations of the Program;
5. Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to these records (e.g., deactivating their passwords and user names);
6. Take all reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect this personal information in the manner provided for in this regulation; and ensure that these third-party service providers are applying personal information protective security measures at least as stringent as those required to be applied to personal information under this regulation;

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP in Minneapolis.
7. Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected, limit the time personal information is retained to that reasonably necessary to accomplish this purpose and limit access to those persons who are reasonably required to know personal information to accomplish this purpose or to comply with state or federal record retention requirements;

8. Identify records, computing systems, and storage media (e.g., laptops and portable devices used to store personal information) to determine which records contain personal information, except where the Program provides for the handling of all records as if they all contained personal information;

9. Implement reasonable restrictions on physical access to records containing personal information (including a written procedure regarding the manner in which physical access to these records is restricted) and store the records and data in locked facilities, storage areas or containers;

10. Regularly monitor to ensure that the Program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrade information safeguards as necessary to limit risks;

11. Review the scope of the security measures at least annually or when there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information;

12. Document responsive actions taken when a data security breach incident occurs and conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to the protection of personal information; and

13. Establish and maintain a security system, covering its computers and any wireless system, for a Covered Entity that electronically stores or transmits personal information, which, at a minimum:

   (A) secures user authentication protocols, including: 1) control of user IDs and other identifiers; 2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies (e.g., biometrics or token devices); 3) control of data security passwords to ensure that these passwords are kept in a location or format that does not compromise the security of the data they protect; 4) restricting access to active users and active user accounts only; and 5) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

   (B) has secure access control measures that: 1) restrict access to records and files containing personal information to those who need personal information to perform their job duties; and 2) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

   (C) to the extent technically feasible, encrypts (i.e., transforms data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key) all transmitted records and files containing personal information that will travel across public networks, and encrypts all data to be transmitted wirelessly;

   (D) has reasonable monitoring of systems for unauthorized use of or access to personal information;

   (E) encrypts all personal information stored on laptops or other portable devices;

   (F) includes reasonably up-to-date firewall protection and operating system security patches for files containing personal information on a system that is connected to the Internet, reasonably designed to maintain the integrity of the personal information;

   (G) has reasonably up-to-date versions of system security agent software, which includes malware protection and reasonably up-to-date patches and virus definitions or a version of this software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and

   (H) educates and trains employees on the proper use of the computer security system and the importance of personal information security.

**ENFORCEMENT**

The statute under which this regulation was issued provides for enforcement by the Massachusetts Attorney General. The MOCABR stated in its “Frequently Asked Qs” that it will discover “who is not playing by the rules when a [data security] breach occurs and it is investigated.”

**NEXT STEPS**

Given the broad application of this regulation and the compliance date of Jan. 1, 2010, an entity needs to determine whether it is a Covered Entity. If so, the Covered Entity must work on preparing and implementing a Program. As part of this Program, the Covered Entity must take all reasonable steps to verify that third-party service providers have the capacity to protect personal information in the manner provided for in this regulation and to ensure that they are applying personal information protective security measures at least as stringent as those required to be applied to personal information under this regulation. Also, the Covered Entity must, to the extent technically feasible, encrypt all transmitted records and files with personal information that will travel across public networks, and encrypt all data to be transmitted wirelessly. Finally, the Covered Entity must encrypt all personal information stored on laptops or other portable devices.
Revised Nevada Privacy Law Furthers Encryption and Payment Card Law Trends

Melissa J. Krasnow, Dorsey & Whitney LLP

Nevada was the first state to enact a law requiring a company that transfers customer personal information outside of its secure system through an electronic transmission (other than a facsimile) to use encryption. This law continues in effect until January 1, 2010. This law was amended and the effective date for the amended law is January 1, 2010. Interestingly, other privacy laws (examples include the Massachusetts written information security program law and the Federal Trade Commission's Red Flags Rule) also were amended during the past year. The amended Nevada law is notable for many reasons. The amended law continues the trend of two newer types of state privacy laws – encryption laws and payment card laws. Massachusetts has a written information security program law that mandates the use of encryption. Minnesota was the first state to enact a payment card law. More specifically, the amended law expands coverage beyond customer personal information to all personal information. The amended law also requires compliance with the Payment Card Industry Data Security Standard. Finally, the amended law provides for relief from damages in the event of a data breach.

Application

The amended law applies to a company doing business in Nevada that deals with nonpublic personal information, except for telecommunication providers. The amended law covers a company outside of Nevada that does business in Nevada. Whether a company does business in Nevada depends on (i) the nature of the company's business in Nevada and (ii) the quantity of business conducted by the company in Nevada.

The definition of “personal information” is from the Nevada data breach law and means an individual's first name or first initial and last name in combination with their (i) Social Security Number (excluding the last four digits), (ii) driver's license number or identification card number or (iii) account number, credit card number or debit card number, together with any required security code permitting access to their financial account, when both the name and the foregoing data element are not encrypted.

Encryption Requirements

There are two encryption requirements under the amended law. A company that does not accept a payment card (a credit card, charge card, debit card or similar card) in connection with a sale of goods or services must use encryption (i) to transfer any personal information through an electronic, nonvoice transmission (other than a facsimile) outside the company's secure system or (ii) when a data storage device (like a computer, cell phone, magnetic tape, electronic computer drive and optical computer drive) containing personal information is moved beyond the company's physical or logical controls. However, the amended law does not apply to data transmission over a secure, private communication channel for the (A) approval or processing of negotiable instruments, electronic fund transfers or similar payment methods or (B) issuance of reports regarding account closure due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.
“Encryption” means the protection of data in electronic or optical form, in storage or in transit, using: (i) an encryption technology that has been adopted by an established standards setting body like the Federal Information Processing Standards issued by the National Institute of Standards and Technology (NIST), that renders the data indecipherable in the absence of associated cryptographic keys necessary to enable decryption and (ii) appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using the guidelines of an established standards setting body such as the NIST.

Payment Card Requirement

A company that accepts a payment card in connection with a sale of goods or services must comply with the current version of the Payment Card Industry Data Security Standard as adopted by the PCI Security Standards Council or its successor organization (PCI DSS), not later than the date for compliance in PCI DSS or by the PCI Security Standards Council or its successor organization. PCI DSS is an industry security standard developed by the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc., with requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. PCI DSS is intended to help organizations proactively protect customer account data.

Liability for Data Breach

A company that (i) complies with the amended law and (ii) suffers a data breach that is not caused by gross negligence or intentional misconduct by the data collector, its officers, employees or agents is not liable for damages.

Conclusion

A company that must comply with the Massachusetts law and the amended Nevada law must reconcile the encryption requirements under these laws. The amended Nevada law is effective January 1, 2010, and the Massachusetts law is effective March 1, 2010. The Massachusetts law requires a company to establish a comprehensive written information security program that contains the encryption requirements, so a company needs to revisit these requirements in light of the encryption requirements under the amended Nevada law. Further, a company that must comply with the Minnesota law and the amended Nevada law must address the payment card requirements of both laws. A company that is subject to the payment card requirement under the amended Nevada law needs to determine the requirements for compliance with PCI DSS.

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP.

1 NRS 597.970.
3 201 CMR 17.00 et seq. and 16 C.F.R. § 681.1.
4 201 CMR 17.00 et seq.
5 Minn. Stat. § 325E.64.
7 Executive Management, Ltd. v. Ticor Title Insurance Co., 38 P.3d 872 (Nev. 2002).
8 NRS 603A.040.
Federal and State Privacy Laws – Compliance Deadlines Fast Approaching

The number and complexity of federal and state privacy laws continue to increase. These laws affect a broad range of public and private companies, including U.S. companies as well as foreign companies that conduct business in the United States.

Any company that possesses personal information relating to U.S. employees, customers, shareholders or others likely is subject to privacy laws. For purposes of the privacy laws, personal information typically includes names together with information like social security numbers, financial account information or driver’s license numbers. Protected health information is covered by the federal Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act.

A number of new privacy law compliance deadlines are fast approaching. Failure to comply with privacy laws could trigger U.S. regulator and State Attorney General action as well as monetary penalties. In some cases, there also could be private lawsuits.

Below is a brief summary of upcoming privacy law compliance deadlines.

**November 1, 2009 – Federal Trade Commission Written Identity Theft Prevention Program**

A company that regularly extends, renews or continues credit, including accepting deferred payments for goods and services, may need to comply with the Federal Trade Commission’s "Red Flags" Rule. Examples of these companies include utility companies, telecommunications companies, finance companies, mortgage brokers, real estate agents, health care providers, lawyers, accountants, other professionals, automobile dealers, retailers that offer financing or collect or process credit applications for third party lenders and third party debt collectors that regularly renegotiate the terms of a debt. This Rule requires that a written identity theft prevention program be in place.

**January 1, 2010 – Nevada Requirements for Encryption**

A company (except for a telecommunications provider) doing business in Nevada that deals with personal information must comply with specific encryption requirements if it does not accept a payment card (a credit card or similar card) in connection with a sale of goods or services. This law also requires that a company that does accept payment cards in connection with a sale of goods or services comply with the current version of the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an industry security standard developed by the PCI Security Standards Council (including American Express, Discover, JCB, MasterCard...
and Visa) for the protection of customer account data.

**February 17, 2010 – Federal HITECH Act Requirements**

Under the federal HITECH Act, health plans, health care providers and health care clearinghouses (i.e., covered entities), among other things, must review and update their business associate agreements, as well as their privacy and security policies and procedures, regarding (i) marketing, (ii) sale of protected health information, (iii) minimum necessary standards, (iv) accounting of disclosures and (v) restrictions on disclosure of services paid out-of-pocket. Business associates (those who perform functions on behalf of, or provide services to, covered entities that involve the use of protected health information) will be directly regulated under the HIPAA privacy and security rules, and must comply for the first time with those rules, including, among other things, a requirement to perform security risk assessments and develop security policies and procedures to address HIPAA security standards.

**March 1, 2010 (Subject to a Revised Version of This Regulation) – Massachusetts Comprehensive Written Information Security Program**

A company that owns or licenses personal information regarding Massachusetts residents must have a comprehensive written information security program with encryption requirements in place. In addition, third-party service providers – by contract – must implement and maintain appropriate security measures for personal information. A company that complies with HIPAA requirements or the Gramm-Leach-Bliley Act also must comply with this regulation. On September 22, 2009, a public hearing on this regulation was held. The Massachusetts Office of Consumer Affairs and Business Regulation expects to issue a revised version of this regulation in the coming weeks.

**We Can Help**

The upcoming compliance deadlines just hint at the many applicable privacy laws that present traps for the unwary. Implementing policies and procedures is not only advisable, but often times required under applicable privacy laws. From data breach notification procedures to record retention policies to social media policies, we can help you navigate the ever-changing landscape of privacy laws. For additional information and updates, please contact Melissa Krasnow at krasnow.melissa@dorsey.com.

**Disclaimer**

©2009 Dorsey & Whitney LLP. This article is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created or continued by reading this article. Members of the Dorsey & Whitney LLP group issuing this communication will be pleased to provide further information regarding the matters discussed therein.