US Privacy and Data Security Law: Overview

by Ieuan Jolly, Loeb & Loeb LLP
Maintained • USA

This Note provides an overview of prominent US privacy and data security laws relating to the collection, use, processing and disclosure of personal information. It summarizes key federal privacy and data security laws, certain state laws, with a focus on California and Massachusetts, and the Mobile Marketing Association and Payment Card Industry Data Security Standards, two key industry-specific privacy and data security guidelines and requirements.

Contents

In the US, there is no single, comprehensive federal law regulating privacy and the collection, use, processing, disclosure and security of **personal information** (also known as personally-identifiable information or PII). Instead, there is a system of federal and state laws and regulations, as well as common law principles, that overlap, dovetail and sometimes contradict one another. In addition, government agencies have developed guidelines and industry groups have undertaken self-regulatory efforts that do not have the force of law but are considered best practices. These self-regulatory programs often have accountability and enforcement components and may refer companies to government regulators such as the Federal Trade Commission (FTC) if the companies fail to comply.

Recent increases in data security breaches have led to an expansion of this patchwork system, which is becoming one of the fastest growing areas of legal regulation. The growth in interstate and cross-border data flow, together with new privacy and data security-related statutes and regulations, heightens the risk of privacy violations and creates a significant compliance

challenge.

In light of these developments, this Note provides an overview of certain key privacy and data security laws. In particular, the Note looks at:

- The consequences of failing to comply with privacy and data security laws.
- The key federal laws in this area, with an explanation of the entities and data covered by the law, the obligations and requirements under the legislation and potential sanctions and liability.
- Certain state laws in California and Massachusetts, where rigorous privacy and data security laws have been adopted.
- Industry guidelines and standards.

Privacy and Data Security Risks

Failure to comply with privacy and data security laws can result in significant adverse consequences, including:

- Government-imposed civil and criminal sanctions, including fines and penalties.
- Significant fines and damages awards resulting from private lawsuits, including class actions (permitted under some privacy and data security laws).
- Damage to the company's reputation and customers' confidence and trust, resulting in lost sales, market share and brand and stockholder value.

The adverse consequences of failing to safeguard personal information can be serious, as the following examples demonstrate:

- **Target Corporation.** In the largest data breach to ever affect a retailer, Target announced in late 2013 that it was affected by a breach that may have resulted in the disclosure of the payment card information of over 40 million consumers and the personal information of an additional 70 million consumers. To date, Target has been sued by consumers and shareholders in over 70 lawsuits in addition to being the subject of multiple regulatory investigations.
- **TJX Companies, Inc.** One of the largest data security breaches in the US cost TJX Companies, Inc., the parent company of several retailers including TJ Maxx and Marshalls, at least $256 million and perhaps up to $500 million. The company discovered in December 2006 that credit and debit card numbers of more than 45 million consumers were stolen and used to make purchases and open fictitious accounts. The company settled several class action lawsuits filed by consumers, as well as lawsuits filed by credit card companies and banks that had to reissue millions of cards.
- **Heartland Payment Systems, Inc.** In January 2009, Heartland Payment Systems, Inc., which provides bank card payment processing services to merchants, announced that hackers had broken into its systems and stolen payment card data. In possibly the largest data breach involving payment cards, an estimated 130 million credit and debit card numbers were stolen.

Federal Laws

There are many federal laws that regulate privacy and the collection, use, processing and disclosure of personal information, including:

- Broad federal consumer protection laws, such as the **Federal Trade Commission Act** (FTC Act), that are not specifically privacy and data security laws, but are used to prohibit unfair or deceptive practices involving the collection, use, processing, protection and disclosure of personal information.
- Laws that apply to particular sectors, such as the:
  - **Gramm-Leach-Bliley Act** (GLBA), which applies to financial institutions; and
  - **Health Insurance Portability and Accountability Act** (HIPAA), which applies to medical information.
- Laws that apply to types of activities that use personal information or might otherwise affect individual privacy, such as the:

- Telephone Consumer Protection Act for telemarketing activities; and
- **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** for commercial e-mail.

In addition, there are many federal security and law enforcement laws that regulate the use of personal information such as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), and federal and state wiretapping laws, but a discussion of these laws is outside the scope of this Note.

This section examines the following key federal privacy laws in more detail:

- FTC Act (regulating unfair or deceptive commercial practices).
- Gramm-Leach-Bliley Act (GLBA) also known as the Financial Services Modernization Act of 1999 (regulating personal information collected or held by financial institutions).
- **Federal Trade Commission's** "Red Flags" Rules issued under the Fair and Accurate Credit Transactions Act (FACTA) (requiring financial institutions and creditors to have written information security programs).
- HIPAA, as amended by the **Health Information Technology for Economic and Clinical Health Act** (HITECH) (regulating **protected health information** (PHI)).
- Certain other prominent federal laws:
  - **Children's Online Privacy Protection Act** (COPPA) (regulating the online collection of information from children);
  - **Fair Credit Reporting Act** (FCRA), as amended by FACTA (regulating consumer credit and other information);
  - CAN-SPAM (regulating commercial e-mail);
  - Telephone Consumer Protection Act (TCPA) (regulating telemarketing);
  - **Electronic Communications Privacy Act** (ECPA) (regulating electronic communications); and
  - **Computer Fraud and Abuse Act** (CFAA) (regulating computer tampering).

Federal Trade Commission Act (FTC Act)

The FTC Act is a federal consumer protection law that prohibits unfair or deceptive commercial practices and has been applied to business practices that affect consumer privacy and data security. The FTC is active in this area and brings enforcement actions against companies, including for:

- Failing to comply with statements made in their posted privacy policies.
- Making material changes to their privacy policies without adequate notice to consumers.
- Failing to provide reasonable and appropriate protections for sensitive consumer information held by them.

The FTC also issues guidelines relating to privacy and data security that are not legally binding but are considered best practices. For example, in March 2012, the FTC issued its final report on consumer privacy protection with recommendations for best privacy practices for companies (see *Protecting Consumer Privacy in an Era of Rapid Change*). In 2009, the FTC issued revised *Self-Regulatory Principles for Behavioral Advertising* (Behavioral Advertising Principles), which set out non-binding guidelines for conducting behavioral advertising (meaning the tracking of an individual's online activities to deliver tailored advertising). The self-regulatory program was expaned in 2015 to the mobile environment.

Entities Subject to the FTC Act

The FTC Act and related FTC-issued rules and guidelines apply to most companies and individuals doing business in the US, other than certain transportation, telecommunications and financial companies that are primarily regulated by other national agencies.

The Behavioral Advertising Principles apply to website operators that engage in behavioral advertising (also called contextual advertising and targeted advertising). Compliance with these principles is voluntary, although many companies adopt them as best practices.

Regulated Data

The FTC Act does not regulate specific categories of personal information. Instead, it prohibits unfair or deceptive acts or practices that affect consumers' personal information.

The Behavioral Advertising Principles apply to entities that track a consumer's online activity to deliver advertising targeted to the consumer's interests.

The Behavioral Advertising Principles apply to data that "could reasonably be associated with a particular consumer or computer or other device" and so is not limited to a more narrow definition of personal information (which is commonly defined as information that can be linked to a specific individual, including but not limited to an individual's name, address, e-mail, Social Security number or driver's license number).

General Obligations

The FTC Act prohibits unfair or deceptive acts or practices. Through broad application of its authority under the Act, the FTC has emerged as the principal federal regulator for privacy and data security.

The FTC has used its authority under the FTC Act to charge companies that:

- Fail to comply with statements made in their posted website privacy policies.
- Make material changes to their privacy policies without adequate notice to consumers.
- Fail to provide reasonable and appropriate protections for personal information held by them.

Notice and Disclosure Requirements

The FTC Act does not expressly require a company to have or disclose a privacy policy. The FTC has taken the position, however, that:

- If a company discloses a privacy policy, it must comply with it.
- It is a violation of the FTC Act for a company to retroactively make material changes to its privacy policy without providing consumers with notice of those changes and the opportunity to opt out of the new privacy policy.

The FTC also enforces COPPA (see *Children's Online Privacy Protection Act (COPPA)*), which requires websites that are directed to children, or that knowingly collect personal information from children, to provide a privacy policy.

The FTC's Behavioral Advertising Principles suggest that website operators engaging in behavioral advertising:

- Disclose to consumers their data collection practices tied to online behavioral advertising.
- Disclose that consumers can opt out of (that is, say "no") these practices.
- Provide a mechanism to the consumer for opting out (for example, by allowing the consumer to electronically check a box indicating that the consumer is opting out or by sending an e-mail to the operator).

Consent Requirements

Although the FTC Act does not expressly address consent, website operators that revise their privacy policies should obtain affirmative express consent (that is, allow consumers to opt-in) before using their data in ways that are materially different from the privacy policy that was in effect when the data was collected.

The FTC also enforces COPPA (see *Children's Online Privacy Protection Act (COPPA)*), which requires websites that are directed to children, or that knowingly collect personal information from children, to obtain "verifiable parental consent" before collecting, using or sharing children's personal information.

The FTC's Behavioral Advertising Principles suggest that website operators obtain affirmative express consent (which can be provided online) from consumers before collecting or using sensitive consumer data in connection with online behavioral advertising. Under the Behavioral Advertising Principles, sensitive data includes (but is not limited to):

- Financial data.
- Data about children.
- Health information.
- Precise geographic location information.
- Social Security numbers.

Individual Access to Collected Data and Right to Correct or Delete Data

Generally, the FTC Act and most US federal and state privacy laws, with some notable exceptions, including HIPAA (see *Health Insurance Portability and Accountability Act (HIPAA)*) and some California laws (see *California Laws*), do not provide individuals with specific rights to access or correct their personal information.

However, COPPA (see *Children's Online Privacy Protection Act (COPPA)*), is enforced by the FTC and requires that website operators allow parents to:

- View the personal information collected by a website about their child.
- Delete and correct that information.

In addition, the White House's 2012 Privacy Report and Consumer Privacy Bill of Rights (which will be the bases for new voluntary codes of conduct) state that, "companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation."

Data Security Requirements

While the FTC Act does not specifically address data security, the FTC has brought enforcement actions alleging that the failure to take reasonable and appropriate steps to protect personal information is an "unfair act or practice" in violation of the FTC Act. For example, the FTC has found violations of the FTC Act where a company:

- Failed to encrypt information while it was in transit or stored on the network.
- Stored personally identifiable information in a file format that permitted anonymous access.
- Did not use readily accessible security measures to limit access.
- Failed to employ sufficient measures to detect unauthorized access or conduct security investigations.
- Created unnecessary business risks by storing information after it had any use for the information, in violation of bank rules.

(See *In the Matter of BJ's Wholesale Club, Inc. 140 FTC 465 (FTC Consent Order, Sept. 20, 2005)*.)

The FTC has taken the position in enforcement actions that inadequate data security practices can form the basis for a claim

of deceptive practices under the FTC Act where a privacy policy states that the business had implemented reasonable and appropriate security measures, see *Federal Trade Commission v. Wyndham Worldwide Corporation, et al. 2:13-cv-01887, D.N.J. (2012).*

The FTC's Behavioral Advertising Principles suggest that website operators that collect or store consumer data for behavioral advertising purposes should:

- Provide reasonable security for that data.
- Retain data for only the time necessary to fulfill a legitimate business or law enforcement need.

The Behavioral Advertising Principles provide that extent and type of protections given to consumer data should be based on the:

- Sensitivity of the data.
- Nature of the company's business operations.
- Types of risk a company faces.
- Reasonable protections available to a company.

Restrictions on Sharing Data with Third Parties

While the FTC Act does not expressly prohibit the sharing of personal information with third parties, the FTC's position is that, if a company discloses a privacy policy (which may include statements regarding the company's information sharing practices), it must comply with it. This includes situations where the privacy policy states that the company will not rent, sell or otherwise disclose personal information to third parties. The FTC may also bring enforcement actions against companies that have unfair or deceptive information sharing practices, even if these companies did not disclose a privacy policy or have not violated their disclosed privacy policies.

Important Exemptions

The privacy rules and guidelines issued by the FTC provide exemptions from privacy requirements for law enforcement purposes.

Enforcement

The FTC is the primary enforcer of the FTC Act (as well as other federal privacy laws, including COPPA, FCRA and FACTA). Actions the FTC can take include:

- Starting an investigation.
- Issuing a cease and desist order.
- Filing a complaint in court.

The FTC also reports to Congress on privacy issues and recommends the enactment of required privacy legislation.

Sanctions and Other Liability

The FTC Act provides penalties of up to $40,000 per offense (increase from $16,000 effective as of Aug. 1, 2016). Criminal

penalties include imprisonment for up to ten years. The FTC can also:

- Obtain injunctions.
- Provide restitution to consumers.
- Require repayment of investigation and prosecution costs.

Settlements with the FTC and other government agencies also often provide for onerous reporting requirements, audits and monitoring by third parties.

Notable examples of FTC enforcement actions include:

- In 2015, Nomi Technologies, a company that tracked consumers' physical locations in stores, agreed to settle FTC charges that it failed to provide an in-store mechanism for opting out of the tracking and failed to tell consumers when they were being tracked in stores.
- In 2015, two data brokers settled FTC charges that they posted unencrypted spreadsheets on the Internet containing consumers' bank account and credit card numbers, birth dates, contact information, employers' names and information about debts the consumers allegedly owed.
- In 2014, Snapchat, a popular social media messaging platform and mobile app, and the FTC announced a settlement of charges that Snapchat allegedly collected geolocation data despite a privacy policy to the contrary, collected users' contacts information from their address books without notice or permission, and failed to protect users' data which led to the hacking of 4.6 million user accounts.
- In 2009, CVS Caremark, operator of the largest pharmacy chain in the US, agreed to pay $2.25 million to settle charges brought by the FTC and the Department of Health and Human Services (HHS) for violating consumer and medical privacy laws.
- In 2008, TJX, Inc., the parent company of several major retailers, in settling charges of failing to adequately protect customers' credit card numbers (see *Privacy and Data Security Risks*), agreed to allow comprehensive audits of its data security system for 20 years.
- In 2006, ChoicePoint, a database owner and data broker, agreed to pay $15 million to settle charges filed by the FTC for failing to adequately protect the data of millions of consumers.

Gramm-Leach-Bliley Act (GLBA)

The privacy and data security provisions of GLBA (also referred to as the Financial Modernization Act) regulate the collection, use, protection and disclosure of non-public personal information by financial institutions.

Entities Subject to GLBA

GLBA applies to:

- "Financial institutions," which is broadly defined to include any institution engaging in "financial activities," including, but not limited to:
  - banks;
  - securities firms;
  - insurance companies;
  - other businesses that may not traditionally be thought of as financial institutions but provide financial services and products, such as:
    - mortgage lenders or brokers;
    - credit counseling services and other financial advisors;
    - collection agencies; and
    - retailers that issue their own credit cards.

- According to the FTC, an institution must be "significantly engaged" in financial activities to be considered a financial institution. Whether a financial institution is significantly engaged in financial activities is a flexible standard that takes into account all of the facts and circumstances.
- Affiliated and unaffiliated third parties that receive non-public personal information from financial institutions.
- Persons who obtain or attempt to obtain non-public personal information from financial institutions through false or fraudulent means.

Regulated Data

GLBA applies to non-public personal information collected by a financial institution that is provided by, results from or is otherwise obtained in connection with consumers and customers who obtain financial products or services primarily for personal, family or household purposes from a financial institution.

Non-public personal information under GLBA generally is any "personally identifiable financial information" that is:

- Not publicly available.
- Capable of personally identifying a consumer or customer.

"Consumers" are individuals who have obtained a financial product or service but do not necessarily have an ongoing relationship with the financial institution (for example, someone who cashed a check with a check-cashing company or made a wire transfer or applied for a loan).

"Customers" are a subset of consumers and refers to anyone with an ongoing relationship with the institution.

General Obligations

GLBA regulates the collection, use, protection and disclosure of non-public, personal information. GLBA requires that financial institutions:

- Notify their customers about their information-sharing practices and provide customers with a right to opt out if they do not want their information shared with certain unaffiliated third parties (GLBA Financial Privacy Rule).
- Implement a written security program to protect non-public personal information from unauthorized disclosure (GLBA Safeguards Rule).

In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and re-disclosure of that information.

Notice and Disclosure Requirements

GLBA requires a financial institution to provide notice of its privacy practices, but the timing and content of this notice depends on whether the subject of the data is a consumer or a customer:

- A customer is entitled to receive the financial institution's privacy notice both:
  - when the relationship is created; and
  - annually thereafter.
- A consumer is entitled to receive the financial institution's privacy notice if the financial institution intends to share the consumer's non-public personal information.

The privacy notice must be a clear, conspicuous and accurate statement of the financial institution's privacy practices. It should describe:

- The categories of information that the financial institution collects and discloses.
- The categories of affiliated and non-affiliated entities with which it shares information.
- That the consumer or customer has the right to opt out of some disclosures.
- How the consumer or customer can opt out (if an opt-out right is available).

In 2009, the FTC (along with the other federal regulatory bank agencies responsible for enforcing GLBA) issued a form model privacy notice. Although financial institutions are not required to use the form, those that do will obtain a "safe harbor" and satisfy the GLBA disclosure requirements for privacy notices. The final *rule and form* are available from the FTC.

Consent Requirements

Although GLBA does not require any affirmative consent from a customer or consumer, GLBA does require a financial institution, at the time of setting up a customer relationship and at least annually thereafter, to:

- Notify customers and consumers of the institution's privacy policy and practices.
- Provide the individual with "reasonable means" to opt out of certain uses and disclosures of the individual's non-public personal information. The means can be written, oral or electronic.

Under GLBA, a financial institution does not need to provide an opt-out right to:

- Share non-public personal information for the purpose of administering or enforcing a transaction that a customer requests or authorizes.
- Share non-public personal information with outside companies that provide essential services, such as data processing or servicing accounts, if certain conditions are met (such as contractually binding the outside company to protect the confidentiality and security of the data).

Individual Access to Collected Data

GLBA allows consumers or customers to opt out of certain disclosures, but generally does not provide affirmative access rights to these individuals.

Restrictions on Disclosing Personal Information to Third Parties

Restrictions under GLBA on disclosing personal information to third parties depends on whether the third party is an affiliate or unaffiliated third party:

- **Disclosures to affiliates.** A financial institution can disclose a consumer's non-public personal information to an affiliated entity if it provides notice of this practice. The financial institution does not need to obtain affirmative consent or provide an opt-out right for this disclosure. An affiliated entity is "any company that controls, or is controlled by, or is under common control with another company" and includes both financial and non-financial institutions.
- **Disclosures to unaffiliated third parties.** Generally, a financial institution must provide notice and a right to opt out of disclosures of personal information to unaffiliated parties. However, a financial institution can disclose an individual's non-public personal information with an unaffiliated entity, without allowing the individual to opt out, if all of the following conditions are met:
  - the disclosure is to a third party that uses the information to perform services for the financial institution;

- the financial institution provides notice of this practice to the individual before sharing the information; and
- the financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only for the prescribed purposes.

Financial institutions may also disclose personal information to unaffiliated third parties without providing an opt-out right under certain circumstances, including where the disclosure is:

- "Necessary to effect, administer or enforce a transaction" or made with the customer's consent.
- For compliance purposes (for example, to an insurance rating organization or credit reporting agency).
- For law enforcement purposes.

Data Security Requirements

The GLBA Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of the customer information it handles. As part of its plan, each company must:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks.
- Implement an identity theft prevention program in connection with "covered accounts."
- Implement regulations requiring the financial institutions to notify the regulator (and in certain cases the customer) when there has been unauthorized access to "sensitive customer information."
- Select service providers that are able to maintain appropriate safeguards, contractually require service providers to maintain safeguards and oversee service providers' handling of customer information.
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations or the results of security testing and monitoring.

The requirements are designed to be flexible. According to the FTC, companies should implement safeguards appropriate to their own circumstances.

Data Breach Notification Requirements

GLBA does not include an explicit data breach notification requirement. However, several of the federal bank regulatory agencies (such as the **Office of the Comptroller of the Currency** and the **Federal Reserve Board**) have implemented regulations requiring financial institutions subject to their authority to notify the regulator (and in some cases the customer) when there has been an unauthorized access to "sensitive customer information."

Sensitive customer information generally includes a customer's name, address or telephone number combined with one or more of the following items of information about the customer:

- Social Security number.
- Driver's license number.
- Account number.
- Credit or debit card number.
- Personal identification number or password that would permit access to the customer's account.

Enforcement

Multiple federal regulatory agencies enforce GLBA, including the **Consumer Financial Protection Bureau** ("CFPB"), the FTC and the federal banking agencies. In addition, state insurance agencies enforce GLBA. For example, the federal banking agencies, the CFPB, the **Securities and Exchange Commission** and the **Commodity Futures Trading Commission** have jurisdiction over banks, **thrifts**, credit unions, brokerage firms and **commodity** traders. The enforcing agency depends not only on the target of enforcement, but also whether it is the Privacy Rule or Safeguards Rule being enforced.

GLBA does not include a right for individuals to bring private actions.

Sanctions and other Liability

Penalties for violations of GLBA are determined by the authorizing statute of the agency that brings the enforcement action. For example, for enforcement actions brought by the FTC, sanctions and other civil and criminal liability include:

- Penalties of up to $40,000 per offense (increase from $16,000 effective as of Aug. 1, 2016).
- Persons and entities who obtain, attempt to obtain, cause to be disclosed or attempt to cause to be disclosed customer information of a financial institution (relating to another person) through a false, fictitious or fraudulent means, can be subjected to fines and imprisoned for up to five years.
- Criminal penalties of up to ten years' imprisonment and fines of up to $500,000 (for an individual) or $1 million (for a company), if the acts are committed or attempted while violating another US law, or as part of a pattern of illegal activity involving more than $100,000 in a year.

For more information on GLBA, see *Practice Note, GLBA: The Financial Privacy and Safeguards Rules*.

Dodd-Frank Wall Street Reform and Consumer Protection Act

In 2010, the **Dodd-Frank Wall Street Reform and Consumer Protection Act** (Dodd-Frank Act) created the CFPB. The Dodd-Frank Act grants the CFPB financial privacy rulemaking and enforcement authority under GLBA (see *Gramm-Leach-Bliley Act (GLBA)*). The Dodd-Frank Act also gives the CFPB enforcement authority against covered organizations that engage in acts or practices related to consumer financial products and services that are:

- Unfair.
- Deceptive.
- Abusive.

(*12 U.S.C. §§ 5531(a), 5536(a)(1)*.)

The CFPB interprets this authority broadly to take data security actions against consumer financial product and service providers. For example, in March 2016, the CFPB announced its first data security action against Dwolla, Inc. for deceptive practices related to representations the company made about its online payment service. In addition to paying a $100,000 monetary penalty, the CFPB's consent order requires Dwolla to:

- Stop misrepresenting its data security practices.
- Develop, implement and maintain a comprehensive written information security plan.
- Properly train employees and fix security flaws.
- Annually obtain and submit to the agency an independent data security program audit.

(See *Legal Update, CFPB's First Data Security Action Imposes $100,000 Penalty*.)

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA governs **individually identifiable health information**. It applies broadly to health care providers, data processors, pharmacies and other entities that come into contact with this information. Relevant HIPAA privacy and data security rules include the:

- Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), which apply to the collection, use and disclosure of PHI. For more information on the Privacy Rule, see *Practice Note, HIPAA Privacy Rule*.
- Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule), which provide standards for protecting PHI. For more information on the Security Rule, see *Practice Note, HIPAA Security Rule*.
- Standards for Electronic Transactions (HIPAA Transactions Rule), which apply to the electronic transmission of medical data.

These HIPAA rules were revised in early 2013 under the HIPAA "Omnibus Rule." Compliance with these changes was required by September 23, 2013. The HIPAA Omnibus Rule also revised the Security Breach Notification Rule (*45 C.F.R. Part 164*), which requires covered entities to provide notice of a breach of protected health information. Under the revised rule, a covered entity must provide notice of acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule, unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised.

Entities Subject to HIPAA

HIPAA applies to "covered entities" and their "business associates." Covered entities include:

- Health plans.
- Health care clearinghouses.
- Health care providers that conduct certain financial and administrative transactions electronically.

A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. These functions and activities include, for example:

- Claims processing and administration.
- Data analysis and processing.
- Quality assurance.
- Billing.
- Benefits management.
- Practice management.
- Re-pricing.

The jurisdictional scope of HIPAA is limited to covered entities over which the US government has enforcement authority. However, certain business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of US jurisdiction.

Regulated Data

HIPAA regulates protected health information (PHI), which is defined as individually identifiable health information that is maintained or transmitted by a covered entity or its business associate.

General Obligations
HIPAA regulates the use and disclosure of PHI and the collection, use, maintenance or transmission of electronic PHI, and requires notice of privacy practices.

HIPAA requires (with some exceptions) that covered entities:

- Use, request and disclose only the minimum amount of PHI necessary to complete a transaction (HIPAA Privacy Rule).
- Implement data security procedures, protocols and policies at administrative, technical, physical and organizational levels to protect PHI (HIPAA Security Rule).
- Comply with uniform standards created for certain electronic transactions (HIPAA Transactions Rule).
- Notify individuals if there is a security breach (and requires that business associates of HIPAA-covered entities to notify these covered entities in the event of a security breach). In late 2009, the FTC issued a similar breach notification rule for companies that are not subject to HIPAA regulations but that develop and distribute online and offline software applications that process personal health records.

Notice and Disclosure Requirements
The HIPAA Privacy Rule requires each covered entity to provide notice to individuals of its privacy practices and of the individuals' rights under HIPAA, generally on the first visit for treatment. The rule sets out specific requirements for the contents and method of the notice.

Consent Requirements
HIPAA generally requires covered entities to obtain consent in writing from an individual subject before using or disclosing that individual's PHI to third parties, with certain exceptions (for example, to provide medical treatment). Consent must generally:

- Be in writing.
- Contain the signature of the individual and the date.

The HIPAA Privacy Rule provides specific statements that must be included in the consent.

With some exceptions (such as the disclosure of psychotherapy notes), HIPAA allows a covered entity to use and disclose PHI without first obtaining consent under certain circumstances, for example, for:

- Medical treatment.
- Payment.
- Healthcare operations.

For a model notice of privacy practices acknowledgment form under HIPAA, see *Standard Document, HIPAA Notice of Privacy Practices Acknowledgment Form*.

Special Rules for Certain Categories of Data

There are specific rules under HIPAA governing the disclosure of "psychotherapy notes." In general, a covered entity must obtain written authorization before disclosing psychotherapy notes, even for purposes of medical treatment, medical operations or payment.

Individual Access to Collected Data
Under HIPAA, individuals have the right (with some exceptions) to:

- Request access to their PHI.
- Make corrections to their PHI.
- Request an accounting of the manner in which their PHI has been used and disclosed.

Restrictions on Sharing Data with Third Parties
HIPAA generally requires covered entities to obtain consent in writing from an individual subject before using or disclosing that individual's PHI to third parties, with certain exceptions (for example, to provide medical treatment).

Covered entities are permitted to disclose PHI to business associates, if the parties enter into an agreement that requires the business associate to:

- Use the information only for the purposes required or permitted by the covered entity.
- Safeguard the information from misuse.
- Help the covered entity to comply with its duties under the Privacy Rule.

When a covered entity has knowledge that its business associate has materially breached or violated the applicable agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, to terminate the contract. If termination of the agreement is not feasible, a covered entity must report the problem to the HHS Office for Civil Rights.

Data Security Requirements
The HIPAA Security Rule requires covered entities to implement data protection policies and reasonable security procedures, including:

- Administrative safeguards, which generally include administrative activities such as assigning responsibility for the security program to the appropriate individuals or requiring security training for employees.
- Physical safeguards, which include physical mechanisms required to protect electronic systems and ePHI, such as limiting facilities to authorized individuals.
- Technical safeguards, which include automated processes designed to protect data and control access, such as using authentication controls and encryption technology.

For more information on the HIPAA Security Rule, see *Practice Note, HIPAA Security Rule*.

Data Breach Notification Requirements
HHS also requires covered entities to notify individuals when their unsecured personal health information has been breached. For more information on the HIPAA breach notification rules, see *Practice Note, HIPAA Breach Notification Rules*.

Important Exemptions
HIPAA does not apply to health information that is:

- Not individually identifiable (for example, aggregate data).
- Used by individuals or entities that do not fall within the definitions of "covered entities" or "business associates" of covered entities. For example, some educational and employment records (for example, a report about an individual's fitness for duty that is used to make an employment decision) would not fall within the scope of HIPAA.

There are many exemptions from the restrictions on disclosure of PHI, for example:

- For law enforcement purposes.
- To avert a serious public health threat.

Enforcement
HIPAA is enforced by the Office of Civil Rights within HHS. This office can initiate investigations into covered entities' information handling practices to determine whether they are complying with the HIPAA Privacy Rule and allows individuals to file complaints about privacy violations. However, HIPAA does not include a right for individuals to bring private actions.

Sanctions and other Liability
HIPAA authorizes the HHS to impose civil penalties ranging from $100 - $1.5 million based on a four-part framework that examines:

- Whether the operator knew of the violation.
- Whether the operator was wilfully negligent.
- Whether the violation was quickly corrected.

In assessing the amount of civil penalties, HHS will also examine certain mitigating or aggravating factors, such as:

- The nature and extent of the violation.
- The nature and extent of the harm.
- The operator's history of compliance.

In addition, HIPAA allows for criminal penalties of up to $250,000 and ten years' imprisonment if the offense was committed under false pretenses or with intent to sell the data for commercial gain.

Other Federal Laws

Children's Online Privacy Protection Act (COPPA)
The FTC is the primary enforcer of COPPA which applies to the online collection of information from children under the age of 13. More specifically, COPPA applies to commercial websites or online services that:

- Are directed to children under 13 and collect personal information from children.
- Have actual knowledge that they are collecting personal information from children.

In December 2012, the FTC issued final amendments to its COPPA Rule that went into effect on July 1, 2013.

Under the amended COPPA Rule, personal information is defined as individually identifiable information about a child that is collected online, such as:

- A full name.
- A home address.
- Online contact information.
- A telephone number.
- A social security number.
- A persistent identifier that can be used to recognize a user over time and across different websites or online services.
- A photo, video or audio file, where such file contains a child's image or voice.
- Geolocation information sufficient to identify a street name and name of a city or town.
- Information concerning the child or the child's parents that an operator collects online from the child and combines with an identifier described above.

COPPA's requirements include, among other things, that these websites or online services:

- Provide a privacy notice on the site (including a clear and prominent link to the notice from the home page and at each area where it collects personal information from children) that states certain required information to inform parents about their information practices.
- Before collecting, using or disclosing personal information of children:
  - provide direct notice to parents (containing the same information required in the website notice); and
  - obtain (with some exceptions) "verifiable parental consent." The method for obtaining consent varies depending on the type of use that will be made.
- On request, provide parents of children who have given personal information with:
  - a description of the types of personal information collected;
  - an opportunity to prevent any further use or collection of information; and
  - reasonable means to obtain the specific information collected.
- Maintain procedures to ensure the confidentiality, security and integrity of the personal information collected.

However, COPPA does include limited exceptions allowing operators to collect certain information without obtaining parental consent in advance, including, for example, to:

- Provide the required privacy notice to the child's parent and seek consent.
- Respond to a one-time request from a child (if the e-mail address is then deleted).
- Respond more than once to a specific request, for example, for a subscription to a newsletter (the operator must notify a parent that it is communicating regularly with the child and give a parent the opportunity to stop the communication before sending or delivering a second communication to the child).
- Protect the safety of a child who is participating on the site (the provider must notify the parent and give an opportunity to prevent further use of the information).
- Protect the security or avoid liability of the site or to respond to law enforcement.

For more information, see *Practice Note, Children's Online Privacy: COPPA Compliance*.

Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA)

A law relating to GLBA, the FCRA, as amended by FACTA limits how consumer reports and credit card account numbers

can be used and disclosed. The FCRA applies to:

- Consumer reporting agencies.
- Those who use consumer reports (such as lenders and employers).
- Those who provide consumer credit information to reporting agencies (such as credit card companies).

As defined in the FCRA, a consumer report is any communication issued by a consumer reporting agency used to evaluate a consumer's eligibility for credit or insurance that relates to a consumer's:

- Credit worthiness.
- Credit history.
- Credit capacity.
- Character.
- General reputation.

FACTA amended the FCRA to, among other things:

- Allow consumers to:
  - receive on request a free credit report once per year from the consumer credit reporting companies; and
  - place fraud alerts on their credit histories to reduce identity theft.
- Restrict businesses (with some exceptions) from printing more than five digits of a consumer's payment card number on receipts provided to the cardholder at the point of sale.
- Create the "Red Flags" Rule (see *The "Red Flags" Rule*).

Rules implemented under FACTA also:

- Require consumer reporting agencies and any other businesses that use consumer reports to adopt procedures for properly disposing of consumer information (the FACTA Disposal Rule).
- Prohibit companies from using certain credit information received from an affiliate to market goods or services to a consumer, unless the consumer is given notice, a reasonable opportunity to opt-out, and a simple and reasonable method for opting-out (the FTC Affiliate Sharing Rule).

The "Red Flags" Rule

The Red Flags Rule issued by the FTC (along with other federal banking agencies) requires "financial institutions" and "creditors" with "covered accounts" (as defined in the rule) to develop a written program that identifies and detects the relevant warning signs, or "red flags" of identity theft. These can include, for example:

- Unusual account activity.
- Fraud alerts on a consumer report.
- Attempted use of suspicious account application documents.

Among other requirements, the program must describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program.

The Red Flags Rule has been in effect since November 1, 2008 for financial institutions and covered entities under the jurisdiction of the federal bank agencies and the National Credit Union Administration. The Red Flags Rule for those financial institutions and covered entities that fall under the FTC's jurisdiction went into effect on December 31, 2010. In April 2013, the SEC and CFTC issued final joint red flag rules and guidelines for entities subject to their enforcement authority effective as of May 20, 2013.

More information on the *Red Flags Rule* is available from the FTC.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
The CAN-SPAM Act regulates the collection and use of e-mail addresses for commercial purposes. CAN-SPAM prohibits senders of commercial e-mails from using:

- Any false or misleading header information.
- Subject lines that would be likely to mislead a recipient about a material fact regarding the contents or subject matter of the message.

Senders of commercial e-mails must also follow certain requirements, including providing in each e-mail, a clear and conspicuous:

- Identification that the message is an advertisement or solicitation.
- Notice of the opportunity to decline to receive further commercial e-mail messages from the sender (an opt-out) and instructions on how to do so.

For more information on CAN-SPAM, see *Practice Note, E-mail Marketing: CAN-SPAM Act Compliance*.

Telephone Consumer Protection Act (TCPA)
The TCPA regulates the collection and use of telephone numbers for commercial purposes. It applies both to telephone calls and text messages. The TCPA and the regulations promulgated under the Act set out rules governing, for example:

- Times during the day when telephone solicitations can be made.
- Use of automated telephone equipment for solicitations.
- Maintenance of a "Do Not Call" registry.
- Information required to be given to the consumer by someone making a telephone solicitation.

New rules went into effect October 2013 that require written consent by the consumer to receive certain communications. For more information on the 2013 amendments, *see Legal Update, New FCC Telemarketing Rule to Become Effective*.

The TCPA permits private rights of action and provides for recovery of either actual damages or statutory damages ranging from $500.00 to $1,500.00 per unsolicited call or message. Because of these statutory damages, TCPA class action litigation has been a key issue for businesses, and the terms of the statute are frequently litigated (see *Practice Note, TCPA Litigation: Key Issues and Considerations*). For more information on the Federal Communication Commission's interpretation of the TCPA regulations, see *Expert Q&A: Far-reaching Declaratory Ruling on the TCPA*.

Electronic Communications Privacy Act (ECPA)
The ECPA governs the interception of electronic communications. It applies to anyone who improperly accesses, intercepts or discloses electronic communications (whether stored or in transit) that affect interstate or foreign commerce. Violations of the ECPA can result in fines, and in some cases, imprisonment.

Computer Fraud and Abuse Act (CFAA)
The CFAA governs computer hacking and makes certain acts regarding the unauthorized access to protected computers

criminal offenses, including:

- Knowingly accessing a computer without authorization to obtain national security data.
- Intentionally accessing a computer without authorization to obtain information:
  - contained in a financial record of a financial institution or contained in a file of a consumer reporting agency on a consumer;
  - from any department or agency of the US; and
  - from any protected computer if the conduct involves an interstate or foreign communication.

The CFAA defines a "protected computer" as a computer that is used in interstate or foreign commerce (that is, any laptop or computer connected to the internet). For more information on the CFAA, see *Practice Note, Cyber Attacks: Prevention and Proactive Responses*.

State Laws

Hundreds of privacy and data security laws governing the collection, use, protection and disclosure of personal information exist at the state level, with inconsistent scope and obligations. State privacy and data security laws include, for example:

- **Baby FTC Acts and other consumer protection statutes.** Like the FTC Act, many states have adopted broad consumer protection statutes that prohibit unfair or deceptive business practices.
- **GLBA and HIPAA add-ons.** GLBA and HIPAA do not preempt more protective state laws concerning the privacy of consumer financial information or personal health information if these state laws are not inconsistent.
- **Social Security number laws.** Many states have adopted specific laws governing the collection, use, protection and disclosure of Social Security numbers.
- **Records disposal laws.** Several states, including California, New Jersey and New York, have enacted laws requiring proper disposal of records containing personal information. For example, California requires businesses to dispose of records containing personal information by shredding, erasing or otherwise modifying the personal information in these records to make it unreadable (*Cal. Civ. Code § 1798.81*).
- **Card transaction laws.** Several states, including California, New York and Massachusetts, have enacted laws that limit the collection of personal information in connection with payment card transactions.
- **Medical information laws.** A number of states, including California, have adopted statutes specifically aimed at the protection of medical information.
- **Data security laws.** Several states, including California and Massachusetts, have enacted laws requiring that companies take certain steps to protect the security of personal information that they collect, use and maintain.
- **Breach notification laws.** California was the first state to enact a data security breach notification law. This law dramatically changed the privacy landscape in the US. Currently, nearly all states and the District of Columbia, Guam, Puerto Rico and the US Virgin Islands have enacted laws requiring notification of security breaches involving personal information. For more information on US data security breach notification laws and practical tips on how to prepare for and respond to a data security breach, see *Practice Note, Breach Notification*.

In addition, a growing number of states have laws that govern social media privacy and the privacy of student records.

Conflicting federal privacy laws preempt some of these laws, which compounds the challenge for companies trying to find a road map for privacy compliance in the US.

Because California and Massachusetts have adopted some of the most rigorous privacy and data security laws to date, this Note provides an overview of:

- California laws relating to:
  - online privacy (California's Online Privacy Protection Act (CalOPPA));
  - required disclosure of information-sharing practices with their customers who request such information (California

"Shine the Light" Law);
  - reasonable data security (California Data Security Law); and
  - breach notification (California's Breach Notification Law).
- Massachusetts's data security regulations requiring businesses to take specific steps to maintain security of personal information of Massachusetts residents (Massachusetts Data Security Regulation).

California Laws

Entities Subject to Regulation

Most states have enacted some form of privacy legislation, but California has traditionally led the way, having enacted multiple privacy laws, some of which have far-reaching effects at a national level. Unlike many US privacy laws, California's resemble the more stringent and comprehensive European approach to privacy protection under the EU Data Protection Directive (see *Box, Cross-border Issues*). California is one of only a handful of states to create and Office of Privacy Protection. California privacy and data protection laws typically:

- Mandate or encourage an opt-in (affirmative consent) standard.
- Provide consumers with the ability to learn how their personal information is used.
- Allow consumers (as individuals or as part of a class) to file enforcement suits.

For more information about these and other California privacy laws, see *Practice Note, California Privacy and Data Security Law: Overview*.

CalOPPA applies to operators of commercial websites and online services that collect personally identifiable information about individual California residents who use or visit the websites or services (*Cal. Bus. & Prof. Code § 22575(a)*). The California Attorney General has stated that this law also applies to mobile apps and has filed enforcement actions relating to mobile app compliance.

The California Breach Notification Law applies to any person or business that conducts business in California and that owns or licenses computerized data that includes personal information.

Regulated Data

CalOPPA defines "personally identifiable information" as individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

- First and last name.
- Home or other physical address, including street name and name of a city or town.
- E-mail address.
- Telephone number.
- Social Security number.
- Any other identifier that permits the physical or online contacting of a specific individual.
- Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described above.

(*Cal. Bus. & Prof. Code § 22577(a)*.)

The California Breach Notification Law regulates "personal information," which means:

- An individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - Social Security number;
  - medical information;
  - health insurance information;
  - driver's license number or California Identification Card number;
  - account number or credit or debit card number, in combination with any required security code, access code or password that would allow access to an individual's financial account; and
  - a user name or e-mail address, in combination with a password or security question and answer that would allow access to an online account.

(*Cal. Civ. Code § 1798.82*.)

However, personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

Notice and Disclosure Requirements

CalOPPA requires commercial websites and online services to disclose their online privacy practices to consumers. Each privacy policy must:

- Identify the categories of:
  - personally identifiable information that the operator collects through the website or online service; and
  - third-party persons or entities with whom the operator may share that personally identifiable information.
- Explain how a consumer can:
  - review his personal information collected by the operator of the website or online service;
  - make changes to that information (if the website or online service operator allows this); and
  - explain how the website or online service operator notifies consumers of changes to its privacy policy.
- State the effective date of the privacy policy.

The privacy policy must be "conspicuously posted" and links to the privacy policy must conform with specific placement and formatting requirements. Further, the Act includes disclosure requirements relating to "do-not-track" mechanisms and online behavioral tracking (*Cal. Bus. & Prof. Code § 22575(b)*).

In addition, under the Privacy Rights for California Minors in the Digital World amendments to the Act, certain website operators are prohibited from advertising and marketing products not legally available to minors (such as alcohol, firearms, tobacco, tattoos and lottery tickets). (*Cal. Bus. & Prof. Code § 22580, et seq.*)

Consent Requirements

CalOPPA requires every commercial website to conspicuously post a privacy policy that describes the information handling procedures of that website but does not specifically require consent to collection or use.

However, other California statutes require express consent when using personal information. For example:

- California's medical privacy law prohibits using personal medical information for direct marketing purposes without consent (*Cal. Civ. Code § 1798.91*).
- California's financial privacy law prohibits sharing or selling personally identifiable non-public financial information without consent (*Cal. Fin. Code §§ 4050-4060*).

Special Rules for Certain Categories of Data
There are several California laws that provide special rules in relation to the use, processing, collection, transmission and disclosure of certain types of data including:

- Financial and medical data.
- Social Security numbers.
- Credit card account numbers.
- Telecommunications records.
- Radio frequency identification (RFID).
- Library records.

Individual Access to Collected Data
The California "Shine the Light" Law allows consumers to learn how their personal information is shared by companies for marketing purposes and encourages businesses to let their customers opt out of this information sharing. In response to a customer's request, a business must provide either of the following:

- A list of the categories of personal information disclosed to other companies for their marketing purposes during the preceding calendar year, with the names and addresses of those companies.
- A privacy statement that gives the customer a cost-free means to opt out of such information sharing.

(*Cal. Civ. Code § 1798.83*.)

Financial services companies subject to the California Financial Information Privacy Act are exempt from this law.

In addition, under the Privacy Rights for California Minors in the Digital World amendments to CalOPPA, if operators of web sites have actual knowledge that a minor is using the site or service, or if the site or service is directed to minors, operators must, among other things:

- Permit a minor to remove or request the removal of certain online content.
- Disclose how minors can remove or request removal of content.

The law does not require companies to remove data from their servers:

- As long as they delete it from their websites.
- If the minor "received compensation or other consideration" for the content.

Restrictions on Sharing Data with Third Parties
Several California statutes include restrictions on sharing data. For example, the California Online Privacy Protection Act requires every commercial website to conspicuously post a privacy policy that describes the information handling procedures of that website and to disclose the categories of third parties with whom personally-identifiable information is shared. In addition, the California Data Security Law, *Cal. Civ. Code § 1798.81.5*, addresses data security as it applies to third parties.

Data Security Requirements
California requires that businesses that own, license or maintain personal information about a California resident implement and maintain "reasonable security procedures and practices" based on the nature of the information to protect that information from unauthorized disclosure. The law does not specifically define what "reasonable" procedures may be.

California law also provides that a business that discloses personal information about a California resident to an unaffiliated third party in connection with a contract must require by contract that the third party:

- Implement and maintain reasonable security procedures and practices appropriate to the nature of the information.
- Protect the personal information from unauthorized access, destruction, use, modification or disclosure.

(*Cal. Civ. Code § 1798.81.5*.)

Breach Notification Requirements

The California Breach Notification Law addresses the requirement to disclose security breaches (*Cal. Civ. Code § 1798.82*). Under certain circumstances, in the event of a data security breach involving personal information, notice must be provided to all affected individuals. This notice may be provided by one of the following methods:

- Written notice.
- Electronic notice, if the notice provided is consistent with national laws regarding electronic signatures (for example, The Electronic Signatures in Global and National Commerce Act).
- Substitute notice, if the company demonstrates one of the following:
  - the cost of providing notice would exceed $250,000;
  - the subject class to be notified exceeds 500,000 persons; and
  - the company does not have sufficient contact information.

Substitute notice must include all of the following:

- E-mail notice when the company has an e-mail address for the subject persons.
- Conspicuous posting of the notice on the company's relevant website page, if the company maintains one.
- Notification through major state-wide media.

The California Breach Notification Law is triggered by the unauthorized disclosure of unencrypted personal information, so it encourages companies to encrypt the personal information of California residents.

However, if a company maintains its own notification procedures as part of an information security policy for the treatment of personal information, and these procedures are otherwise consistent with the timing requirements of the law, the company will be in compliance with the notification requirements if it notifies the subject persons of a breach in accordance with its policies.

The disclosure of a security breach required by the California Breach Notification Law may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

In addition, the law provides additional requirements in the event of a data breach, including content requirements for any notices, requirements relating to credit monitoring offers and requirements for regulatory reporting. For more information on California's data breach law, see *State Q&A, Data Breach Notification Laws: California*. For more information on US data security breach notification laws generally, see *Practice Note, Privacy and Data Security: Breach Notification*.

Student Privacy

The California Student Online Personal Information Protection Act (SOPIPA) goes into effect January 2016 (to be codified at *Cal. Bus. and Prof. Code §22584* (S.B. 1177)). SOPIPA will prohibit an operator of an website, online service, online application or mobile applications from:

- Knowingly engaging in targeted advertising to students or their parents or legal guardians.
- Using covered information to amass a profile about a K–12 student.
- Selling a student's information, or disclosing covered information.

Additionally, SOPIPA will require an operator to:

- Implement and maintain reasonable security procedures and practices.
- Protect covered information from unauthorized access, destruction, use, modification or disclosure.
- Delete a student's covered information on request of a school or district.

Once effective, SOPIPA will be the nation's most stringent student privacy protection statute.

Enforcement

The California Online Privacy Protection Act and the California Breach Notification Law are enforced by the California Attorney General and state district attorneys.

Massachusetts Data Security Regulation

The Massachusetts Data Security Regulation, *Mass. Regs. Code tit. 201 § 17.01-17.05*, effective as of March 1, 2010, contains the most rigorous data security requirements imposed on businesses by a state to date.

Entities Subject to Regulation

The Massachusetts Data Security Regulation applies to all businesses (whether located in or outside of Massachusetts) that own, license, store or maintain personal information about Massachusetts residents (*Mass. Regs. Code tit. 201 § 17.01*).

Regulated Data

The Massachusetts Data Security Regulation defines "personal information" as:

- A Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following elements that relate to that resident:
  - Social Security number;
  - driver's license number or state-issued identification card number; and
  - financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

"Personal information" does not include information that is lawfully obtained from:

- Publicly available information.
- Federal, state or local government records lawfully made available to the general public.

(*Mass. Regs. Code tit. 201 § 17.02*).

General Obligations
The Massachusetts Data Security Regulation requires all persons and entities that own, license, store or maintain personal information about a Massachusetts resident to:

- Develop, implement and maintain a comprehensive, written information security program.
- Implement physical, administrative and extensive technical security controls, including the use of encryption.
- Verify that any third-party service providers that have access to personal information can protect that information.

Data Security Requirements
The Massachusetts Data Security Regulation requires all persons that own, license, store or maintain personal information about a Massachusetts resident to:

- Develop, implement and maintain a comprehensive, written information security program.
- Implement physical, administrative and extensive technical security controls, including the use of encryption.
- Provide for a comprehensive, written information security program that must include safeguards which are appropriate to the:
  - size, scope and type of business of the person obligated to safeguard the personal information under that comprehensive information security program;
  - amount of resources available to that person;
  - amount of stored data; and
  - need for security and confidentiality of both consumer and employee information.

The safeguards contained in this program must be consistent with the safeguards for protection of personal information and information of a similar character set out in any state or federal regulations by which the person who owns or licenses that information may be regulated (*Mass. Regs. Code tit. 201 § 17.03*).

The security controls must cover computers, including any wireless system, and, to the extent technically feasible, must have the following elements:

- Secure user authentication protocols including:
  - control of user IDs and other identifiers;
  - a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - control of data security passwords to ensure that these passwords are kept in a location and/or format that does not compromise the security of the data they protect;
  - restricting access to active users and active user accounts only; and
  - blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
- Secure access control measures that:
  - restrict access to records and files containing personal information to those who need that information to perform their job duties; and
  - 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.
- Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly.
- Reasonable monitoring of systems, for unauthorized use of or access to personal information.
- Encryption of all personal information stored on laptops or other portable devices.
- For files containing personal information on a system that is connected to the internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- Reasonably up-to-date versions of system security agent software which must include 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.
- Education and training of employees on the proper use of the computer security system and the importance of personal information security.

(*Mass. Regs. Code tit. 201 § 17.04*).

Restrictions on Sharing Data with Third Parties
The Massachusetts Data Security Regulation requires oversight of third-party service providers by:

- Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the regulations and any applicable federal regulations.
- Requiring those third-party service providers by contract to implement and maintain appropriate security measures for personal information. However, the Massachusetts Data Security Regulation provides a safe harbor for contracts entered into before March 1, 2010. Contracts entered into before this date will be deemed to satisfy this requirement until March 1, 2012, even if the contract does not include a requirement that the third-party service provider maintain these appropriate safeguards.

(*Mass. Regs. Code tit. 201 § 17.03(2)(f)*.)

Enforcement
The Massachusetts Data Security Regulation is enforced by the Massachusetts Attorney General.

For more information on the Massachusetts Data Security Regulation, see *Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation.*

Industry Guidelines and Standards
In addition to laws, guidelines issued by many industry groups issue guidelines that are generally considered best practices in those industries (such as the payment card, mobile marketing and online advertising industries), or are required by contract, but do not have the force of law. In addition, some industry organizations have implemented enforcement programs (see, for example, *Legal Update, Digital Advertising Alliance Will Enforce Mobile Self-regulatory Program*). Significant examples of self-regulatory regimes include:

- Mobile Marketing Association Guidelines.
- The Payment Card Industry Data Security Standard (PCI DSS).

Mobile Marketing Association Guidelines
The Mobile Marketing Association's *Code of Conduct for Mobile Marketing* (registration required), suggests that mobile marketers (that is, companies advertising on mobile or wireless devices):

- Ask for and obtain an explicit opt-in for all mobile messaging programs.
- Implement a simple opt-out process and reasonable technical, administrative and physical procedures to protect user information from unauthorized use, disclosure or access.

More *information* on the Code of Conduct for Mobile Marketing is available from the Mobile Marketing Association.

Payment Card Industry Data Security Standard

PCI DSS requires all entities that process, store or transmit cardholder data to comply with 12 basic security requirements, including requirements applicable to:

- Firewalls.
- Access controls.
- Monitoring and testing networks.
- Vendor-supplied default passwords.
- Maintaining an information security policy.
- Encryption (the requirement that entities generally have the most difficulty complying with).

PCI DSS is not law. It is an industry standard disseminated and enforced by a group of major credit card brands through contractual obligations. While the individual card companies maintain their own security programs, these programs are consistent with the PCI DSS. Merchant/acquiring banks that wish to process a certain credit card brand's cards become "members" of the individual card institutions. These members are contractually obligated to comply with the PCI DSS and are directly responsible to the card institutions for monitoring and reporting on the PCI compliance of the merchants for whom they process credit card transactions. In turn, these banks are required by the applicable card institutions to contractually oblige their merchants to comply with the PCI DSS. Failures to comply with the PCI DSS can result in significant fines and penalties.

For more information on the card payment system and the PCI DSS requirements, see *Practice Notes, The Card Payment System* and *PCI DSS Compliance*.

Cross-border Issues

There are few limits on the transfer of personal information to countries outside the US. While several US states have enacted laws that limit or discourage outsourcing of data processing beyond US borders, these laws typically apply only to state government agencies and their private contractors. The position of the FTC and other US regulators is that:

- US laws and regulations still apply to the personal information after it leaves the US.
- The regulated entities in the US remain responsible for exported personal information and for the processing of personal information overseas by subcontractors.
- Entities should use the same protections (for example, the use of security safeguards, protocols, audits and contractual provisions) whether the regulated data is located in the US or elsewhere.

However, US businesses that operate multi-nationally must also comply with the data protection laws in each jurisdiction in which they operate. For example, in contrast to US law, in many European countries, privacy is a fundamental individual right, and each EU member state has implemented comprehensive national data protection legislation under the European Union Directive 95/46/EC (EU Data Protection Directive). For an overview, see *Practice Note, Overview of EU Data Protection Regime*.

In addition to providing EU residents with greater data privacy protection and rights to access and control the use of their personal information, the EU Data Protection Directive restricts the transfer of EU personal information to countries outside of the EU that are not deemed to offer "adequate protections" for data privacy (which includes the US) unless certain additional requirements are complied with.

A discussion of data protection laws in other jurisdictions is outside the scope of this Note. For more information on data protection and privacy laws in various jurisdictions, see *Multi-jurisdictional Guide: Data Protection*.

