Information is generated about and collected from individuals at an unprecedented rate in the ordinary course of business. In most cases, this abundance of data is used to increase convenience and efficiency in operations. The primary cost to consumers, clients, and individual employees for this convenience is information privacy—in order to provide better services to clients and employees, companies need certain information about them. Retailers collect addresses, phone numbers, and payment card numbers in exchange for shipping products directly to consumers. Healthcare service providers maintain medical records in exchange for personalized and informed care procedures. Companies collect bank account numbers in exchange for facilitating employee compensation.
There are risks involved in all of this information exchange, and in part because of these risks, there exists a body of law at the federal and state level that addresses the importance of personal information protection, and the security and confidentiality obligations of organizations that collect personal information. The payment card industry maintains its own security standards as well, requiring compliance from payment card companies, affiliated banks, merchants, and payment card processors. This article addresses a selection of some of the laws that address privacy—it is not an exhaustive analysis—and notes that development of privacy legislation is ongoing.

STATE LEGISLATION

The most prominent privacy regulations at the state level are breach notification laws, which set out how companies should provide notification to individuals whose personal information is reasonably believed to have been compromised or exposed in a data security breach of the company. Forty-seven (47) states currently have breach notification laws in place, as well as the District of Columbia, Puerto Rico, the Virgin Islands, and Guam.

Generally speaking, these laws require notification as soon as reasonably possible, consistent with measures to determine the nature and scope of the breach and to restore integrity to the system. In some cases these laws allow for delays in notification at the request of law enforcement agencies in connection with criminal investigations. Most states permit email notification and state-wide media broadcast notification in place of personalized written or telephonic notification once specific thresholds of affected persons or of notification-related expenses are surpassed. Common exceptions included in these laws are for compliance with other laws addressing privacy, or in the event that a company has an internal notification policy that is functionally equivalent to or stricter than the state regulation. Many states require notification to consumer reporting agencies if a privacy breach results in a sufficiently high number of affected individuals, considering the risk of identity theft and potential need for the freezing or correction of consumer credit reports.

CALIFORNIA: CA CIVIL CODE §1798.82

California was the first state to pass a law addressing personal information privacy. The law, passed in 2003, requires state agencies, or persons or businesses conducting business in California, that own or license personally identifiable information (PII) to disclose any breach of security of data to any California resident whose unencrypted PII may have been acquired by an unauthorized person or party. This law was recently amended to define PII as additionally inclusive of user names or email account addresses in combination with the passwords or security questions and answers that would grant access to such accounts.

MASSACHUSETTS: 201 CMR 17.00

STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Massachusetts adopted these regulatory standards, for necessary protective measures of entities that own or license PII of residents, to work alongside the state’s breach notification law in order to better protect personal information. The regulations require development, implementation, and maintenance of a comprehensive information security program, including:
Privacy Legislation and Industry Security Standards

- Dedicated personnel
- Ongoing employee training
- Policies for remote access and transport of records
- Disciplinary measures for noncompliance and violations
- Oversight for third party service providers
- Continual monitoring and review of the program’s utility and effectiveness

Such information security programs are also required to include technical policies focused on software and system maintenance, including secure user authentication protocols, secure access control measures, encryption for transmission, firewalls, and up-to-date security software.

TEXAS: B.C. CODE §§521.002, 521.053 AND S.B. 1610

There is some controversy and question around the Texas privacy breach notification law, in that it has quite broad language regarding who should be notified and under what state’s law. The law requires notification from an entity conducting business in Texas to any individual whose PII may have been acquired by an unauthorized party—even if the individual is a resident of a state that does not have privacy breach notification legislation. This law also allows an entity that conducts business in Texas to provide notification to an individual who is the resident of another state that does have privacy breach notification legislation under that state’s legislation or under the Texas statute.

MINNESOTA: PLASTIC CARD SECURITY ACT

Minnesota has legislation specifically related to breaches where “access device”—payment card—information is exposed. The Minnesota law holds a company that suffers a breach liable for costs related to card reissuance, account closures and openings, refunds to cardholders for any unauthorized transactions related to breached access devices, notification to cardholders, and damages paid by a financial institution for injury of a cardholder as a result of a breach. This law is seen as a codification, in some ways, of the Payment Card Industry Data Security Standards, described below.

FEDERAL LEGISLATION

There is a great deal of federal legislation addressing different kinds of protected information and different industry responsibilities toward protected information and the maintenance of consumer privacy. The laws below were selected for discussion based on reference to them in state breach notification laws as pertaining to the definition and regulation of protected personal information.

GRAMM-LEACH-BLILEY ACT

Under this Act, financial institutions are obligated to respect the privacy of their customers as well as protect the security and confidentiality of those individuals’ nonpublic personal information. In the Act, nonpublic personal information is defined as: “personally identifiable financial information provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution.”
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The Health Insurance Portability and Accountability Act (HIPAA), amended and added to by the Health Information Technology for Economic and Clinical Health Act (HITECH), requires entities that maintain and/or transmit health information to have and uphold administrative, technical, and physical safeguards to ensure the integrity and confidentiality of said information. HIPAA also requires entities maintaining and/or transmitting health information to protect against threats to and unauthorized use of such information.

The information expressly protected by HIPAA is known as individually identifiable health information, defined as: “any information, including demographic information, collected from an individual, that (A) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (B) relates to past, present, or future physical or mental health or condition of an individual, the provision of healthcare to any individual, or the past, present, or future payment for the provision of healthcare to an individual, and – (i) identifies the individual; or (ii) with respect to which there is reasonable basis to believe that the information can be used to identify the individual.” The protection extends to the above kind of information that is transmitted or maintained in electronic media or any other form or medium.

HIPAA, as amended, has its own notification requirements of covered entities that discover they have had a breach, requiring such entities to notify potential affected persons no later than 60 days post-discovery of breach and requiring the notification of media sources if more than 500 individuals’ records are compromised.

FAIR AND ACCURATE CREDIT TRANSACTION ACT

The Fair and Accurate Credit Transaction Act (FACTA) includes Red Flag Guidelines—financial institutions and creditors are to establish reasonable policies and procedures for implementing guidelines regarding identity theft, to identify possible risks to account holders or customers.

IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT

This Act, known also as ITERA, mandates that offenders under the provisions of the act must pay an amount equal to the value of time reasonably spent by the victim in his or her attempt to remediate the intended or actual harm incurred by the victim from the offense. ITERA, as such, puts value on the time and energy factor of the aftermath of identity theft, allowing for remuneration of the victim for his or her efforts to reestablish the security of his or her identity.

FEDERAL TRADE COMMISSION ACT, SECTION 5

The FTC has stepped up as the primary federal regulator when it comes to incidents of data breach. The Commission takes its mandate with regard to data security from Section 5 of its founding legislation, which prohibits “unfair or deceptive acts or practices in or affecting commerce.” The Commission poses that in certain cases, massive data breaches constitute deceptive practices when it comes to organizations’ representations about their data security capabilities. The FTC has investigated several organizations in the aftermath of breach events, requiring extensive corrective action plans in many cases as well as occasionally imposing fines on companies related to breaches.
The Payment Card Industry self-regulates in terms of data security. The stated goal of the PCI-DSS is the enhancement of cardholder data security, through the establishment of baselines of technical and operational requirements designed to protect said data. These standards apply to all entities involved in payment card processing, including merchants, processors, acquiring banks, issuers of payment cards, service providers, and other entities that store, process, and transmit cardholder data. There are six major areas that the requirements fall under:

- Building and maintaining a secure network
- Protecting cardholder data
- Maintaining a vulnerability management program
- Implementing strong access control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy

Non-compliance with the PCI-DSS carries fees and assessments developed by the payment brands currently participating in the PCI-DSS (MasterCard, Visa, American Express, Discover, etc.), where the assessments are levied against merchants or acquiring banks as per their specific merchant service agreements with the payment card companies.

COSTS OF COMPLIANCE

Playing by the rules of these governmental and industry-based regulations often involves some expense, and costs skyrocket if companies are found to be non-compliant with the appropriate regulatory statutes. FACTA, HIPAA/HITECH, and Massachusetts 20 CMR 17.00 all have robust requirements regarding the policies a business should implement in order to protect sensitive information, and the development and maintenance of these policies is a continual expense for entities covered under these statutes. The PCI-DSS also mandates certain security procedures of entities involved in payment card processing. For companies that need to build up their information security from scratch—as they are new organizations, or organizations transitioning into greater integration of digital technologies—coming into compliance with the appropriate regulatory standards can be expensive.

State, federal, and industry regulatory statutes include various fines and penalties for non-compliance with their provisions, and can also require following certain remediation steps in the aftermath of a non-compliance-exposing breach. Companies found to be deficient in their information security policies and procedures have been compelled to obtain biennial audits from independent third parties, over decades in some cases, and have had corrective action plans imposed upon them, all at the companies’ own expense. These case-by-case penalties do not carry standard price tags, and this is a degree of financial uncertainty that any organization would be wise to avoid, however possible. Companies can protect themselves to some extent from exposure to regulatory scrutiny and punishment through the maintenance of compliant information security procedures, or through transfer of part of their risks to an insurer with the purchase of a network security and privacy insurance policy with coverage for regulatory fines and penalties.
CONTINUING REGULATORY DEVELOPMENTS

There have been proposals for a federal security breach notification law that would streamline the requirements of the various state laws and standardize notification procedures in the event of a data breach. With recent large data breaches in the news and at the forefront of public consciousness, proposals for federal legislation have gained traction, and there are several pieces of legislation up for review that address cyber security and security breach notification.

FOR MORE INFORMATION

For further information on the topic of this article, or on cyber exposures and cyber insurance, please feel free to contact Susanne Murray or Fred Podolsky of the Executive Risk Group of Alliant Insurance Services, Inc. The Executive Risk Group of Alliant specializes in all executive risk liability exposures and corresponding executive risk insurances, including directors and officers liability, cyber and privacy, employment practices, fiduciary, professional liability (errors and omissions), and fidelity insurance.

Susanne Murray
Executive Vice President
Executive Risk Group
smurray@alliant.com
212 895 0260

Fred Podolsky
Executive Vice President
Executive Risk Group
fpodolsky@alliant.com
212 895 0261

Cara Murray
Cyber Specialist
Executive Risk Group
cmurray@alliant.com
212 895 0257