Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation

MELISSA J. KRASNOW, VLP LAW GROUP LLP

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note discussing written information security programs (WISPs) under the Massachusetts data security regulation (201 Code Mass. Regs. 17.01). This Note also discusses reasons for adopting a WISP, preliminary considerations, and the Massachusetts Attorney General's enforcement actions.

The Massachusetts data security regulation (201 Code Mass Regs. 17.01 to 17.05) (Massachusetts Regulation) contains some of the most stringent and detailed state-level data security requirements for organizations. Massachusetts was the first state to enact this type of regulation and is one of the few states to require covered organizations to adopt a comprehensive written information security program (WISP) that incorporates specific security measures. The regulation has extensive reach, purporting to cover every organization, wherever located, that owns or licenses Massachusetts residents' personal information.

This Note focuses on developing and implementing WISPs based on the Massachusetts Regulation's requirements. It discusses:

- Preliminary considerations and steps when developing a WISP.
- The Massachusetts Regulation's requirements.
- Massachusetts enforcement actions.

For an example of a WISP that complies with the Massachusetts Regulation and other similar laws, see Standard Document, Written Information Security Program (WISP) (W-001-0073).

REASONS FOR ADOPTING A WISP

In addition to the Massachusetts Regulation, other laws and industry standards may require organizations to develop WISPs and implement reasonable security measures (see Box, Additional Relevant US Laws, Guidance, and Industry Standards and Practice Note, State Data Security Laws: Overview (W-002-2498)). However, even where WISPs are not legally required, they are a good business practice for any organization that collects, uses, stores, transfers, or disposes of personal information.

A well-developed and maintained WISP can provide benefits, including:

- Prompting the business to proactively assess risk and implement measures to protect personal and other sensitive information.
- Establishing that the organization takes reasonable steps to protect personal and other sensitive information, especially in the event of a security incident where litigation or enforcement action could occur. The Federal Trade Commission (FTC) follows a reasonableness standard for data security and its recent enforcement actions demonstrate these expectations. For more on FTC data security guidance and enforcement actions, see Practice Note, FTC Data Security Standards and Enforcement (8-617-7036).

Because of the ongoing threat of data breaches and other cyber incidents, and the potential for significant associated legal, business, and reputational costs, organizations often require their third-party service providers and other business partners to have comprehensive WISPs (see Third-Party Service Providers).

Organizations also increasingly seek cyber liability insurance. Insurers often demand detailed information about an organization's information security program and may require a WISP (see Practice Note, Cyber Insurance: Insuring for Data Breach Risk (2-588-8785)).

PRELIMINARY CONSIDERATIONS

Preliminary steps in developing and implementing a WISP include:

- Identifying reasons for adopting the WISP and the program's objectives (see Reasons for Adopting a WISP).
- Determining, evaluating, and identifying conflicts in the requirements of:
  - the Massachusetts Regulation and all other applicable laws;
  - guidance from governmental authorities;
  - enforcement actions; and
  - industry standards.

- Gathering all relevant information concerning the personal information the organization collects, uses, stores, and shares. This includes identifying:
  - the categories and types of personal information;
  - how the organization collects, uses, stores, transfers, and destroys personal information, and the systems and technologies the organization uses for these purposes;
  - the residences of the individuals whose personal information the organization holds, including US states and any non-US locations;
  - the organization's third-party service providers and other business partners that have or may have access to personal information the organization holds or controls;
  - the organization's current information security procedures, practices, and policies; and
  - the employees within the organization who are responsible for developing, implementing, maintaining, and enforcing the WISP.

For a sample questionnaire counsel can use to assess an organization's personal information collection and handling practices, see Standard Document, Privacy Audit Questionnaire (W-004-1417).

SCOPE OF THE WISP

The scope and complexity of a WISP varies depending on the organization's specific circumstances. However, two threshold issues include whether to:

- Adopt a WISP that applies to:
  - the personal information of only Massachusetts residents; or
  - all personal information the organization holds.
- (See Personal Information Covered by the WISP.)
- Combine the WISP with other information security compliance program documents or maintain separate resources (see Combining with Other Privacy and Information Security Compliance Program Documents).

PERSONAL INFORMATION COVERED BY THE WISP

The organization must initially decide whether to create the WISP to:

- Specifically comply with the Massachusetts Regulation and only apply to Massachusetts residents' personal information.
- Broadly apply to the collection of personal information from Massachusetts residents and others.

Adopting a WISP that applies to all personal information the organization holds can provide administrative ease. Most states do not specifically require organizations to create a WISP. However, a comprehensive WISP reflects best practices and can help reduce the organization's risks by demonstrating that it takes reasonable steps to protect personal information. The organization may choose to use the Massachusetts Regulation as a baseline when creating its program, but should also ensure its WISP takes into account all relevant states' privacy and data security laws, including the various definitions of personal information each state has adopted. For more details on state-specific definitions of personal information, especially as applied in state data breach notification laws, see Practice Note, State Data Breach Laws Protected Personal Information Chart: Overview (4-609-2845).

Conversely, the organization may wish to limit the scope of its WISP to the Massachusetts Regulation to narrow its compliance obligations. For example, where only one business unit of an organization collects Massachusetts residents' personal information, the organization may seek to keep that unit's compliance obligations separate from its other business units' obligations.

COMBINING WITH OTHER PRIVACY AND INFORMATION SECURITY COMPLIANCE PROGRAM DOCUMENTS

Where an organization is subject to more than one set of privacy and information security requirements, it can be administratively simpler to consolidate its programs and related policies and procedures into one comprehensive compliance program document. However, the organization may need to consider potentially conflicting legal requirements. For example, organizations subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Gramm-Leach-Bliley Act (GLBA) must also comply with the Massachusetts Regulation.

Like the Massachusetts Regulation, the GLBA Safeguards Rule requires that financial institutions develop comprehensive WISPs to protect customer information (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules: Information Security Program (4-578-2212)). However, the GLBA Safeguards Rule and Massachusetts Regulation differ in their specific WISP requirements, for example:

- The Safeguards Rule applies only to customer information while the Massachusetts Regulation applies to Massachusetts residents' personal information, including both customer and employee information.
- The Safeguards Rule's requirements are broader and less precise than the Massachusetts Regulation's requirements.

One advantage in keeping a WISP developed specifically for the Massachusetts Regulation separate from the organization's other information security policies is that if the Massachusetts Attorney General or another state attorney general or regulator requests a copy of the Massachusetts WISP, the organization may be able to limit its disclosure to the Massachusetts WISP and not its other policies.

For an example of a WISP that addresses multiple federal and state requirements in one program document, including the Massachusetts Regulation and the Safeguards Rule, see Standard Document, Written Information Security Program (WISP) (W-001-0073).

MASSACHUSETTS REGULATION: GENERAL WISP REQUIREMENTS

The Massachusetts Regulation requires every legal person that owns or licenses personal information about a Massachusetts resident to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that are appropriate to:

- The size, scope, and type of the person's business.
- The person's available resources.
- The amount of stored data.
- The need for security and confidentiality of both consumer and employee information.

In addition, the safeguards must be consistent with any state or federal regulations that apply to that person and require safeguards to protect personal and similar information.

(201 Code Mass. Regs. 17.03(1).)

The Massachusetts Regulation also includes a set of:

- Specific WISP requirements (see Massachusetts Regulation: Specific WISP Requirements).
- Computer system security requirements for organizations that electronically store or transmit personal information (see Massachusetts Regulation: Computer System Security Requirements).

The Massachusetts Office of Consumer Affairs and Business Regulation provides guidance on developing a WISP in its Compliance Checklist and Frequently Asked Questions.

SCOPE

The Massachusetts Regulation applies to any legal person including, for example, a corporation, association, partnership, or other legal entity that owns or licenses Massachusetts residents' personal information. Covered organizations include any that receive, store, maintain, process, or otherwise have access to personal information either for:

- The provision of goods or services.
- Employment.

(201 Code Mass. Regs. 17.02.)

The Massachusetts Regulation applies regardless of whether the person or organization is located in Massachusetts or even the US.

Those who must comply with HIPAA or the GLBA also must comply with the Massachusetts Regulation.

DEFINITION OF PERSONAL INFORMATION

The Massachusetts Regulation defines personal information as a Massachusetts resident's first name or initial and last name combined with one or more of that resident's:

- Social Security number.
- Driver's license number or state-issued identification card number.
- 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 the resident's financial account.

The definition excludes any information lawfully obtained from either:

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

(201 Code Mass. Regs. 17.02.)

MASSACHUSETTS REGULATION: SPECIFIC WISP REQUIREMENTS

The Massachusetts Regulation requires that every comprehensive WISP include:

- Designating one or more employees to maintain the WISP (see Program Oversight).
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of electronic, paper, or other records containing personal information.
- Evaluating and improving, where necessary, the effectiveness of current safeguards for limiting these risks, including:
  - ongoing employee training, including training for temporary and contract employees;
  - employee compliance with policies and procedures; and
  - means for detecting and preventing security system failures.
- (See Identifying and Minimizing Reasonably Foreseeable Internal and External Risks.)
- Developing security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises.
- Imposing disciplinary measures for violations of the WISP's rules.
- Preventing terminated employees from accessing records containing personal information.
- Overseeing service providers by:
  - taking reasonable steps to select and retain third-party service providers capable of maintaining appropriate security measures to protect personal information consistent with the Massachusetts Regulation and any applicable federal regulations; and
  - contractually requiring them to implement and maintain these security measures.
- (See Third-Party Service Providers.)
- Reasonable restrictions on physical access to records containing personal information, and storage of those records in locked facilities, storage areas, or containers.
- Regular monitoring to ensure that the WISP is operating in a way reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.
- Upgrading information safeguards as necessary to limit risks.
- Reviewing the scope of the security measures:
  - at least annually; or
  - whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- Documenting:
  - responsive actions taken in connection with an incident involving a security breach;
  - mandatory post-incident review of events; and
  - any actions taken to make changes in business practices related to protecting personal information.

(201 Code Mass. Regs. 17.03(2).)

PROGRAM OVERSIGHT

The Massachusetts Regulation specifically requires covered organizations to designate one or more employees as the data security coordinator or coordinators to maintain the WISP. The data security coordinators are responsible for ensuring that the WISP's specific requirements are carried out, whether by them or others (see Massachusetts Regulation: Specific WISP Requirements). The considerations in designating data security coordinators and assigning their specific responsibilities depend on the organization's specific circumstances and may include:

- The organization's:
  - size;
  - industry; and
  - regulators.
- The types of personal information that the organization owns or maintains on behalf of another organization.
- The employees responsible for the organization's compliance with security requirements, including compliance with:
  - internal policies;
  - contracts; and
  - relevant laws and industry standards.

The organization should also consider the appropriate business units to involve in program oversight, which may include:

- Legal.
- Information technology.
- Privacy or a broader compliance unit.

IDENTIFYING AND MINIMIZING REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS

A key requirement of the Massachusetts Regulation is identifying reasonably foreseeable internal and external risks and adopting steps to mitigate those risks. Risks vary depending on the organization's specific circumstances. Examples of common risks include:

- Inadequate personnel training (see Inadequate Personnel Training).
- Unencrypted personal information (see Unencrypted Personal Information).
- Personal information in paper format (see Personal Information in Paper Format).
- Lack of control over portable devices (see Lack of Control Over Portable Devices).

For additional examples of common information security gaps that may create risk, see Common Gaps in Information Security Compliance Checklist (3-501-5491).

Inadequate Personnel Training

Inadequate training and education of an organization's personnel creates a reasonably foreseeable internal risk to the protection of personal information. To minimize risk, organizations should ensure that:

- Personnel actually receive training on the proper use of the computer system, the importance of personal information security, and the elements of the WISP, and have access to information about the requirements.
- They have the means to identify when personnel miss or fail to complete the training.
- The training and information sufficiently convey the data security requirements so that personnel can comprehend them.
- They periodically assess compliance.

An organization should provide ongoing training and information and update them as necessary or appropriate. For example, after a data breach or incident, an organization should:

- Update training and information to include lessons learned.
- Consider additional or interim training.

Unencrypted Personal Information

Unencrypted personal information is a reasonably foreseeable risk. The Massachusetts Regulation requires, to the extent technically feasible, encryption of all:

- Transmitted records and files containing personal information that travel across public networks.
- Data containing personal information that is transmitted wirelessly.
- Personal information stored on laptops or other portable devices.

(See Massachusetts Regulation: Computer System Security Requirements.)

To reduce risks caused by unencrypted personal information, an organization can, for example:

- Conduct an initial inventory of all laptops and other portable devices and continuously maintain the inventory. The inventory should identify whether each device is owned by the organization or the individual.
- Determine whether personal information is stored on the laptops and other portable devices and, if so, whether and how the information is encrypted.
- Where technically feasible, implement encryption of personal information when it is stored on portable devices or transmitted over public or wireless networks.
- Implement tools such as data loss prevention software that flag emails containing designated personal information.
- Conduct ongoing training, make regular assessments, and follow up on unsatisfactory results.

The Massachusetts Office of Consumer Affairs and Business Regulation advises against sending unencrypted personal information through email. It suggests instead using alternative methods to conduct transactions involving personal information, for example, by setting up a secure website.

Personal Information in Paper Format

Creating, maintaining, transferring, and disposing of personal information in paper format creates reasonably foreseeable internal and external risks. Examples of records containing personal information often maintained in paper format include:

- Employment-related documents.
- Customer credit card information.
- Tax, employee benefit, and transaction-related documents for the organization's security holders (for example, stockholders or bondholders).

Organizations that handle personal information in paper format must follow appropriate safeguards, which may differ from those for personal information stored in electronic form. These safeguards may include, for example, requiring:

- Storage of paper records containing personal information in a secure location, for example, in locked filing cabinets, and limiting access to these records to specified individuals.
- Using envelopes or mailing covers without transparent windows for mailings that involve content containing personal information.
- Using a cross-cut shredder on paper records before disposal and ensuring disposal is made in accordance with applicable law, internal policies, and procedures (for example, records retention policies) and any contractual requirements.

Lack of Control Over Portable Devices

An organization's lack of control over portable devices creates reasonably foreseeable internal and external risks. Examples of lack of control over portable devices include failing to:

- Inventory and account for portable devices, whether owned by the organization or individually-owned and used for business purposes (see Standard Document, Bring Your Own Device to Work (BYOD) Policy (1-521-3920)).
- Develop policies and procedures regarding use of portable devices for business purposes.
- Properly implement and enforce policies and procedures concerning portable devices.

The Massachusetts Regulation specifically requires organizations to:

- Develop security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises (see Massachusetts Regulation: Specific WISP Requirements).
- Create and maintain a security system covering the organization's computers, including any wireless system (see Massachusetts Regulation: Computer System Security Requirements).

THIRD-PARTY SERVICE PROVIDERS

The Massachusetts Regulation requires that the WISP include oversight of third-party service providers, including contractually requiring third-party service providers to implement and maintain appropriate measures for protecting personal information. Organizations should:

- Conduct data security due diligence on their third-party service providers (see Due Diligence).
- Include specific requirements in third-party service provider agreements involving personal information that address the Massachusetts Regulation and other data security matters (see Key Contract Requirements).
- Monitor their service providers for ongoing compliance and enforce their contractual agreements, as necessary.
- Conduct ongoing training for personnel with responsibility for the organization's third-party service provider contracts to ensure that they are aware of and comply with the Massachusetts Regulation.

For more details on managing vendor privacy and data security issues, see Practice Note, Managing Privacy and Data Security Risks in Vendor Relationships (W-001-8814).

Due Diligence

Organizations should conduct due diligence on their third-party service providers' information security practices. Due diligence should include requesting and reviewing information on:

- The third-party service provider's data security and disaster recovery policies and procedures.
- Data security audit reports concerning the third-party service provider's information security program.
- Details of any actual or potential security breaches or incidents impacting the third-party service provider.

The organization should also consider speaking with existing clients of the third-party service provider.

For a sample questionnaire that organizations can use to assess a vendor's privacy and data security policies, processes, and practices, see Standard Document, Vendor Due Diligence: Security and Privacy Questionnaire (W-011-7859).

Key Contract Requirements

The Massachusetts Regulation requires organizations to contractually obligate their third-party service providers to implement and maintain appropriate measures for protecting personal information. Generally, the organization should consider contract provisions that address:

- General and specific security requirements and procedures that the third-party service provider must maintain.
- The third-party service provider's ongoing compliance with applicable privacy and data security laws, including the Massachusetts Regulation.
- The organization's right to audit the third-party service provider's security procedures and policies.
- The organization's right to:
  - terminate the contract for security-related material breaches; and
  - seek other remedies, for example, indemnification for losses arising out of the third-party service provider's failure to comply with its data security obligations.
- Secure disposal or return of the personal information to the organization on the agreement's termination or expiration.
- Requirements if the third-party service provider suspects or experiences a breach or an incident, such as immediately notifying the organization.

For sample contract clauses, see Standard Clauses, Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer) (2-505-9027).

Organizations may need to amend existing contracts to ensure compliance with the Massachusetts Regulation. Organizations should closely monitor responses to their requests to amend existing contracts and track the status of third-party service provider contracts.

MASSACHUSETTS REGULATION: COMPUTER SYSTEM SECURITY REQUIREMENTS

The Massachusetts Regulation sets out requirements for computer security that, as a practical matter, apply to most organizations. If an organization stores or transmits personal information electronically,

its WISP must include establishing and maintaining a security system that covers its computers, including any wireless system, and at a minimum includes, to the extent technically feasible:

- 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, like biometrics or token devices;
  - control of data security passwords to ensure they are kept in a location 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 accounts after multiple unsuccessful attempts to gain access or limiting access for the particular system.
- Secure access control measures that:
  - restrict access to records and files containing personal information to those who need the information to perform their jobs; and
  - assign to each person with computer access unique identifications and passwords, which are not vendor-supplied default passwords and that are reasonably designed to maintain the integrity and security of the access controls.
- Encryption of all:
  - transmitted records and files containing personal information that will travel across public networks;
  - data containing personal information to be transmitted wirelessly; and
  - personal information stored on laptops or other portable devices.
- Reasonable monitoring of systems for unauthorized use of or access to personal information.
- Reasonably up-to-date firewall protection and operating system security patches for files containing personal information on systems that are connected to the internet, reasonably designed to maintain the integrity of the personal information.
- Reasonably up-to-date versions of system security agent software that includes malicious software (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.
- Employee education and training on the proper use of the organization's computer system security and the importance of personal information security.

(201 Code Mass. Regs. 17.04.)

MEANING OF TECHNICALLY FEASIBLE

The Massachusetts Regulation requires implementation of its computer system security requirements only if they are technically feasible. According to guidance from the Massachusetts Office of Consumer Affairs and Business Regulation, technically feasible means that if there is a reasonable means through technology to accomplish a required result, the organization must use it.

ENCRYPTION

Under the Massachusetts Regulation, encryption means the transformation of data into a form where meaning cannot be assigned without the use of a confidential process or key. The data must be altered into an unreadable form. Password protection that does not alter the condition of the data is not encryption. The definition of encryption is intended to be technology neutral and take into account new developments in encryption technology.

ADDITIONAL RELEVANT US LAWS, GUIDANCE, AND INDUSTRY STANDARDS

Other relevant US laws, guidance, enforcement actions, and industry requirements include:

- **GLBA.** The GLBA Safeguards Rule requires financial institutions to develop a comprehensive written information security program to protect customer information (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules (4-578-2212)).
- **HIPAA.** The Security Rule establishes standards to protect electronic protected health information that is created, received, used, or maintained by a covered entity or a business associate (see Practice Note, HIPAA Security Rule (5-502-1269)).
- **State data security laws.** In addition to Massachusetts, some other states have laws requiring organizations to develop, implement, and maintain reasonable security practices and procedures regarding personal information. For examples and information on other state data security laws, including those with specific information security program requirements, see Practice Note, State Data Security Laws: Overview. States have also enacted sector-specific laws and regulations that impose further data security obligations for some industries. For more regarding state insurance data security laws based on the National Association of Insurance Commissioners (NAIC) Model Insurance Data Security Law (MDL-668), see Practice Note, NAIC Model Data Security Law and State-Specific Implementations (W-020-5945).
- **State guidance.** In February 2016, the California Attorney General issued Data Breach Report 2012-2015 with recommendations defining a baseline level of information security (see Practice Note, California Privacy and Data Security Law: Overview: Regulatory Guidance (6-597-4106)). Specifically, the California Attorney General deems failing to implement minimum information security controls, as defined by the 20 controls in the Center for Internet Security's Critical Security Controls, as a lack of reasonable security.
- **FTC enforcement actions.** The FTC has brought data security enforcement actions under Section 5 of the FTC Act against organizations for failing to take reasonable security measures. As part of its settlements of these enforcement actions, the FTC has required the organizations to implement comprehensive information security programs (see Practice Note, FTC Data Security Standards and Enforcement: Box, Representative FTC Data Security Actions (8-617-7036)).

- **FTC guidance.** The FTC guidance entitled Protecting Personal Information: A Guide for Business describes steps organizations can take to protect personal information and articulates principles for sound data security plans. The FTC's report, Start with Security: A Guide for Business, provides organizations with practical lessons gleaned from its data security enforcement actions. The FTC's report Internet of Things: Privacy & Security in a Connected World also describes security best practices for companies developing connected devices (see also Practice Note, The Internet of Things: Key Legal Issues: Data Security (W-002-6962)).
- **National Institute of Standards and Technology (NIST) guidance.** The NIST cybersecurity framework, Framework for Improving Critical Infrastructure Cybersecurity, developed under Executive Order 13636, is a voluntary risk-based set of industry standards and best practices that organizations can use in managing cybersecurity risks (see Practice Note, The NIST Cybersecurity Framework (5-599-6825)).
- **Payment Card Industry Data Security Standard (PCI DSS).** These data security standards apply to organizations that process, store, or transmit cardholder data. The requirements include protecting cardholder data and maintaining an information security policy (see Practice Note, PCI DSS Compliance (8-608-7192)).

For more information on additional laws, guidance, and industry standards, see Practice Note: US Privacy and Data Security Law: Overview (6-501-4555).

MASSACHUSETTS ATTORNEY GENERAL ENFORCEMENT ACTIONS

If an organization experiences a data breach involving a Massachusetts resident's personal information, it must provide written notification of the data breach to:

- The Massachusetts Attorney General.
- The Massachusetts Office of Consumer Affairs and Business Regulation.
- The affected Massachusetts residents.

The Massachusetts Attorney General can request a copy of the organization's WISP. Massachusetts's data breach notification law also requires organizations to include information on whether they maintain a WISP in their notices to authorities (M.G.L. c.93H §3(b)). For more information on data breach notification requirements in Massachusetts, see State Q&A, Data Breach Notification Laws: Massachusetts (1-578-9413).

The Massachusetts Attorney General has brought a number of enforcement actions relating to data breaches, including participating in multistate actions (for example, see Legal Update, Equifax to Pay $575 Million to Settle Data Breach Claims with FTC, CFPB, and State AGs (W-021-3927)). The enforcement actions show the importance of having a WISP in place and ensuring compliance.

Typically, the actions have alleged that organizations violated one or more of the following laws:

- The Massachusetts Regulation.
- The Massachusetts Security Breach Act (M.G.L. c. 93H, §§ 1 to 6).
- The Massachusetts Consumer Protection Act (M.G.L. c. 93A, §§ 1 to 11).
- HIPAA.

The enforcement actions have included allegations about the organization's failure to:

- Institute security measures, such as encrypting personal information.
- Properly oversee third-party service providers.
- Follow their own WISPs.

Many enforcement actions have resulted in settlement agreements. The settlement agreements have typically required the organizations to take actions such as:

- Institute or comply with a WISP that meets the Massachusetts Regulation's requirements.
- Institute specific security measures, such as:
  - encryption;
  - workforce training; or
  - oversight of third-party service providers.
- Review or audit their security programs.
- Implement specific corrective actions.
- Report to the Massachusetts Attorney General.
- Pay a civil penalty.

Some example enforcement actions include:

- Online sock retailer Bombas LLC agreed to pay $85,000 regarding a data breach, maintain a written information security program, and institute reasonable safeguards for customers' personal information (Office of Massachusetts Attorney General: Press Release, Online Sock Retailer Resolves Claims of Violating Data Security Laws (Aug. 12, 2019)).
- Premera Blue Cross settled for $10 million in a multistate action resolving allegations that its data security failures led to a cyberattack exposing over 10 million consumers' personal information (see Office of Massachusetts Attorney General: Press Release, Health Insurer to Pay $10 Million in National Settlement Over Data Breach Affecting Sensitive Information of Millions (Jul. 11, 2019)).
- Service provider CoPilot Provider Support Services Inc. settled for $120,000, agreeing to update its security policies following its alleged failure to provide timely notice of a data breach (Office of Massachusetts Attorney General: Press Release, Healthcare Services and IT Provider Resolves Data Breach Affecting Nearly 1,900 Massachusetts Residents (Jul. 2, 2019))

- Neiman Marcus's multistate $1.5 million settlement, which resulted from the company's alleged failure to report a 2013 data breach (see Office of Massachusetts Attorney General: Press Release, AG Healey Joins $1.5 Million Multistate Settlement With Neiman Marcus Over 2013 Data Breach (Jan. 8, 2019)).
- McLean Hospital's paid $75,000 and agreed to implement new security and training programs after exposing individuals' personal and health information (see Office of Massachusetts Attorney General: Press Release, McLean Hospital to Implement New Security and Training Programs After Data Breach Exposed Sensitive Health Information (Dec. 19, 2018)).
- Yapstone Holdings Inc. settled for $155,000 to resolve allegations it violated consumer protection and data security laws exposing individuals' personal information (see Office of Massachusetts Attorney General: Press Release, Payment Processor to Pay $155,000 Over Data Breach Affecting Thousands of Massachusetts Residents(Dec. 19, 2018)).
- Uber's multistate $148 million settlement, which resulted from the company's failure to promptly report a data breach (see Office of Massachusetts Attorney General: Press Release, AG Healey Leads Multistate Coalition in Reaching $148 Million Settlement With Uber Over Nationwide Data Breach (Sept. 26, 2018)).
- UMass Memorial Medical Group Inc. and UMass Memorial Medical Center Inc.'s $230,000 payment to resolve claims related to two data breaches exposing personal and health information (see Office of Massachusetts Attorney General: Press Release UMass Memorial Health Care Entities to Pay $230,000 to Resolve AG's Lawsuit Over Data Breaches (Sept. 20, 2018)).
- In one of its early cases, demonstrating the state's intent to pursue cross-border enforcement of the Massachusetts Regulation and HIPAA, the Women and Infants Hospital in Rhode Island agreed to pay $150,000 and take specific compliance steps to resolve allegations that it failed to secure and report the loss of more than 12,000 Massachusetts residents' personal information and protected health information on 19 lost unencrypted backup tapes. (*Commonwealth v. Women & Infants Hosp.*, CIF No. 14-2332G (Mass. Super. Jul. 22, 2014).)

02-20