Massachusetts Data Security Regulations:

New Rules And Old Lessons

Barbara Anthony
Undersecretary of Consumer Affairs
and Business Regulation

Greater Boston Chamber of Commerce
November 9, 2009

Office of Consumer Affairs & Business Regulation

Better businesses. Smarter consumers.

- **THE WRITTEN INFORMATION SECURITY PROGRAM**
- **SPECIAL REQUIREMENTS FOR ELECTRONICALLY STORED INFORMATION**

Office of Consumer Affairs & Business Regulation

"PERSONAL INFORMATION" - WHAT IS IT?

- First name (or initial) and last name

  - Plus -

- SSN,
- Driver's license (or state-issued ID), or
- Financial account number or credit/debit card (with or without pin, password etc.) that would permit access to a MA resident's financial account.

THE WRITTEN INFORMATION SECURITY PROGRAM

- The WISP must be appropriate for the size, scope and type of business, resources available, the amount of data stored, and the need for security and confidentiality of both consumer and employee information;
- The WISP must include administrative, technical, and physical safeguards for PI protection

Office of Consumer Affairs & Business Regulation

WISP (continued)

- The WISP is applicable to paper, electronic and other records, computing systems, and storage media, including laptops and portable devices, that contain PI; and there must be a designated responsible employee;
- Evaluation of reasonably foreseeable internal and external risks to PI, and current safeguards;
- Employee training, and monitoring of employee compliance;

WISP (continued)

- WISP must have policies and procedures for storage, access and transportation of PI off premises;
- Third Party Service Providers: Due diligence related to capacity of TPSP to implement and maintain security measures consistent with these regulations; and a contractual obligation to do so; 2yr. grace period for contracts signed prior to March 1, 2010;

Office of Consumer Affairs & Business Regulation

WISP (continued)

- Regular monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary; annual review or whenever there are changes in business practices;
- Documentation of actions taken in response to a breach of security;

Office of Consumer Affairs & Business Regulation

COMPUTER SYSTEM SECURITY REQUIREMENTS

- The technical feasibility requirement
- Encryption has a technology neutral definition

SYSTEM SECURITY (continued)

SECURE AUTHENTICATION PROTOCOLS:

- Control of user IDs and other identifiers;
- Reasonably secure method of assigning/selecting passwords, or use of unique identifier technologies (such as biometrics or token devices);
- Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- Restriction of access to PI to active users and active user accounts;
- Blocking access after multiple unsuccessful attempts to gain access;

SYSTEM SECURITY (continued)

- Secure access control measures that restrict access, on a need-to-know basis, to PI records and files;
- Assignment of unique identifiers plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls;

SYSTEM SECURITY (continued)

Encryption

- Encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly;
- Encrypt all PI stored on laptops or other portable devices;

Office of Consumer Affairs & Business Regulation

SYSTEM SECURITY (continued)

- Monitoring to alert you to the occurrence of unauthorized use of or access to PI;
- Reasonably up-to-date firewall protection on systems connected to the Internet; and operating system security patches to maintain the integrity of the PI;
- Reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security virus definitions;
- Employee training on the proper use and importance of your computer security system.

Office of Consumer Affairs & Business Regulation

Case Example #1

Premier Capital Lending

December 2008 – FTC Safeguards Rule Case

- Texas-based mortgage lender allowed a third-party home seller to access sensitive consumer data. A hacker compromised the data simply by using the mortgage lender's log-in and accessed hundreds of consumer reports in **unencrypted** form. *Premier* violated its own data security policy; had it followed it, no such data breach would likely have occurred. *Premier* did not assess the risks of allowing a third-party to access credit reports. It also failed to use readily available information to detect signs of unauthorized activity. The hacker was able to obtain *Premier's* user name and password to gain access to at least 400 credit reports.
- The FTC ultimately settled with *Premier*. The settlement contained numerous provisions and lasts for twenty years. *Premier* was required to hire an independent third-party security professional to review their newly established security program every other year for the entire twenty years.

Office of Consumer Affairs & Business Regulation

Case Example #2

Compgeeks.com/Genica Corporation

February 2009 – FTC Section 5 Case

This online seller of computer supplies and electronics failed to securely store sensitive consumer data, including first and last names, telephone and credit card numbers, as well as those cards' expiration dates and security codes. The data was stored in **unencrypted** text on the corporate computer network. Hackers repeatedly exploited the vulnerabilities of *Compgeeks*' website and network data storage and accessed sensitive information, which allowed the hackers to make fraudulent purchases.

Compgeeks also had a data security policy, claiming it "use[d] secure technology, privacy protection controls, and restrictions on employee access in order to safeguard your information." *Compgeeks* parent company, *Genica Corporation*, was also named as respondent in the FTC complaint. The FTC also settled with *Compgeeks* requiring the company to develop a comprehensive security program and contained a ten year monitoring provision.

Office of Consumer Affairs & Business Regulation

Case Example #3

BJ's Wholesale Club, Inc.

2005 – Unfairness Case Under FTCA

- On June 16, 2005, the FTC settled a case against BJ's Wholesale Club, Inc.
- The FTC charged that BJ's had failed to take appropriate security measures to protect the sensitive information of thousands of its customers.
- Stolen credit card and debit card information from BJ's was used by an unauthorized person or persons to make counterfeit credit cards and then to make millions of dollars of fraudulent purchases.
- This failure in security was found to be "unfair" to consumers.

Office of Consumer Affairs & Business Regulation

BJ's Wholesale Club

- Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce.
- Previously, the FTC's privacy and data security cases had been based on "deception," holding companies responsible for failing to abide by their own privacy policies.
- The BJ's case was the first of the FTC's recent privacy and security cases brought under the "unfairness" doctrine.
- BJ's was charged with unfair practices that:
  - Caused substantial injury,
  - Were not reasonably avoidable by consumers, and
  - Were not outweighed by offsetting benefits to consumers or competition.
- The FTC found that BJ's failure to adequately protect individuals' private information was unfair.

BJ's engaged in a number of practices which, taken together, did not provide reasonable security for sensitive customer information.

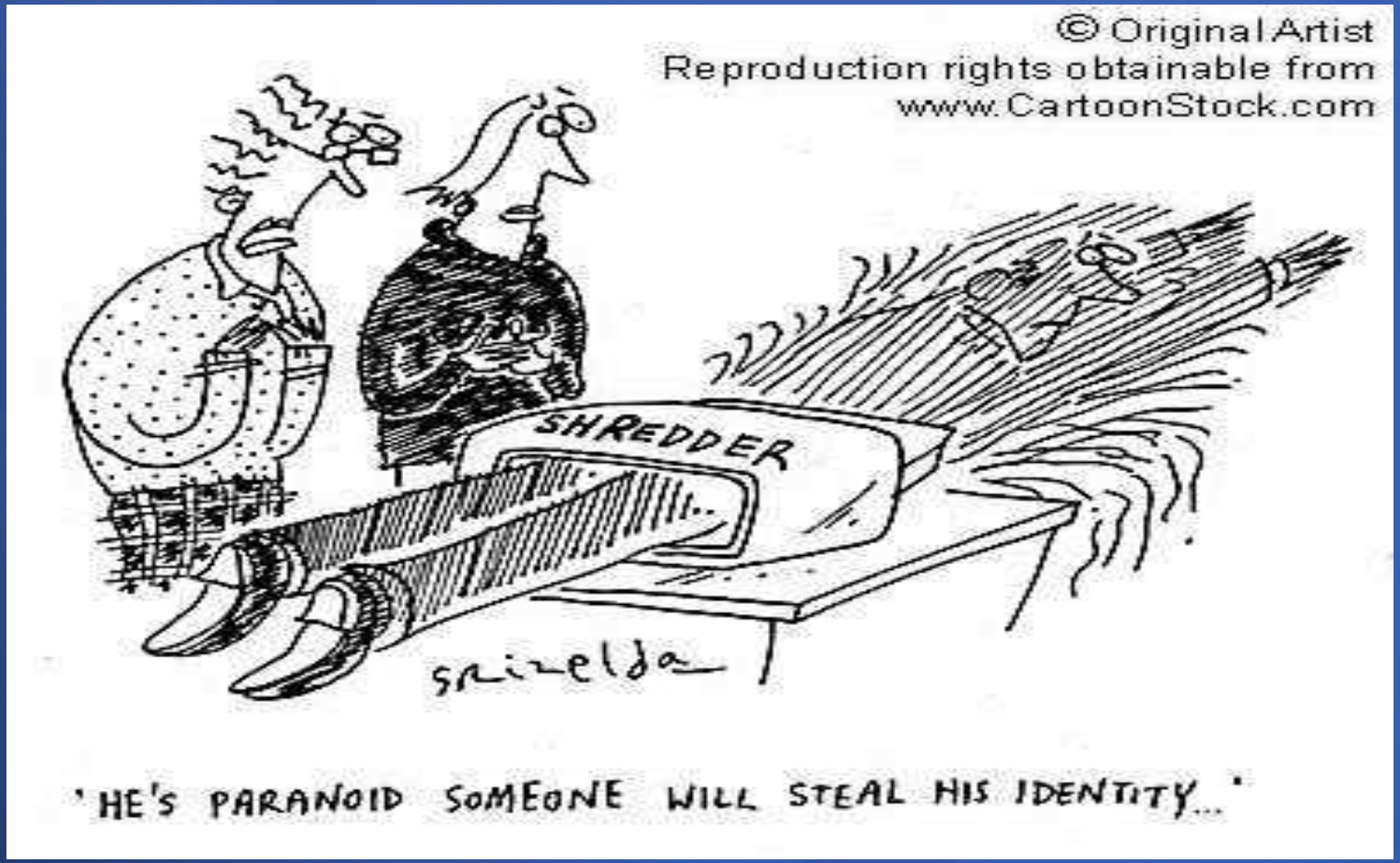
Specifically, they:

- **Failed to encrypt** consumer information, that was taken from the magnetic stripe on credit cards, when it was transmitted or stored on computers in BJ's stores;
- Created unnecessary risks to information by storing it for up to 30 days, in violation of bank security rules, even when it no longer needed the information;
- Stored the information in files that could be accessed using commonly known default user IDs and passwords;
- Failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and
- Failed to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations.

Office of Consumer Affairs & Business Regulation

BJ's Wholesale Club was Required To:

- Refrain from any future violations of the Safeguards Rule; AND…
- Implement a comprehensive information security program; AND…
- Report any change in the corporation that may affect its compliance obligation; AND…
- Allow the FTC to inspect and copy any documents that relate to this matter for a period of five years; AND…
- Obtain and submit audits by an independent third party security professional every other year for *20 years.*


© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
SHREDDER
'HE'S PARANOID SOMEONE WILL STEAL HIS IDENTITY...'

Case Example #4

Designer Shoe Warehouse

2005 - FTC Section 5 Unfairness Case

Until at least March 2005, DSW engaged in a number of practices that taken together failed to provide reasonable and proper security for personal information collected in its stores.

- DSW created unnecessary risk to information, that was taken from the magnetic stripe on credit cards, by storing it in multiple files when it no longer had a business need to keep the information.
- DSW did not use readily available security measures to limit access to its computer networks through wireless access points.
- DSW stored information in unencrypted files that were easily accessible.
- DSW did not limit the ability of computers on one in-store network to connect to computers on other in-store and corporate networks.
- DSW failed to employ sufficient measures to detect unauthorized access.

DSW Settlement Requirements

- DSW Inc. must maintain a comprehensive security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.
  - A risk assessment must occur within employee training, information systems, and potential outside intrusions to the system.
- The company must obtain initial and biennial assessments and reports from an independent qualified third-party professional.
  - Reports shall cover the first 180 days after service of order and each two year period thereafter for 20 years

Office of Consumer Affairs & Business Regulation

Case Example #5

In Re Nations Title Agency

May 2007 – Violations of FTC Privacy Rule, Safeguards Rule and Section 5 of FTCA

- Nations Holding Co. (Kansas). Nations Title Agency (subsidiary) NTA: provides home financing services.
- NHC's Privacy Policy: "physical, electronic, and procedural safeguards"
- *But, what really happened with respect to PI from loan applications?*

- According to KCTV Channel 5 in Kansas City, the **unencrypted** PI was thrown into an unsecured dumpster.

FTC Allegations → NHC failed to:

- Assess risks stored to collected info
- Implement reasonable procedures for employee screening and handling PI
- Implement reasonable security against hackers
- Employ adequate measures to detect and respond to unauthorized PI access: and
- Provide adequate oversight for service providers' handling of PI
- Alleged Violations: Safeguards Rule, Privacy Rule, FTC Act. (Too early for Disposal Rule, 6/05)

Office of Consumer Affairs & Business Regulation

Case Example #6

American United Mortgage

December 2007 – Violations of FTC Safeguards, FTC Privacy and FTC Disposal Rules

- The FTC's complaint alleges that Illinois-based American United Mortgage Company violated the Disposal, Safeguards, and Privacy rules by failing to properly dispose of credit reports or information taken from credit reports, failing to develop or implement reasonable safeguards to protect customer information, and not providing customers with privacy notices.
- As a result of the company's failures, the complaint alleges, on multiple occasions documents containing consumers' personal information were found in and around a dumpster, near its office, that was unsecured and easily accessible to the public. In February 2006, hundreds of such documents were found, many in open trash bags, including consumer reports for 36 consumers. In March 2006, FTC staff notified the company in writing about this situation, and on at least two occasions afterward, more such documents were found in and around the same dumpster.

American United Mortgage

- American United settled with the FTC and paid $50,000 in penalties for violations of the FITC Disposal Rule
- Order prohibits further violations of the Privacy Rules
- American United required to perform independent audit every two years for 10 years

Office of Consumer Affairs & Business Regulation

Case Example #7
Eli Lilly
January 2002 – Deceptive Case under FTCA

- From March 15, 2000 until June 22, 2001, Lilly offered to consumers taking prozac the "Medi-messenger" e-mail reminder service. This service allowed individuals to design and receive email messages reminding them to refill their prescriptions; the emails were individualized and did not disclose anyone's identity to another Medi-messenger user.

- However, in June of 2001 a Lilly employee sent Medi-messenger users an e-mail announcing the termination of their service. The e-mail message included all of the recipients' e-mail addresses within the "To:" line of the message, thereby unintentionally disclosing to each individual subscriber the e-mail addresses of all 669 Medi-messenger subscribers.

Eli Lilly

- Despite this email, Lilly claimed that it employed measures and took steps appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through its web sites. Lilly's privacy policies included statements such as, "Eli Lilly and Company respects the privacy of visitors to its Web sites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource.“

- The FTC complaint alleged that Lilly's claim of privacy and confidentiality was deceptive because Lilly failed to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information, which led to the company's unintentional June disclosure of Medi-messenger subscribers' personal information (*i.e.*, e-mail addresses).

Eli Lilly

Eli Lilly agreed to settle Federal Trade Commission charges regarding the unauthorized disclosure of sensitive personal information collected from consumers through its Prozac.com Web site. As part of the settlement, Lilly agreed to take appropriate security measures to protect consumers' privacy.

The Consent Agreement that Eli Lilly entered into is to last for *twenty years*. Additionally, for the first five years after signing the Agreement Eli Lilly agreed to make available to the FTC for inspection and copying various documents, including consumer-targeted advertising and information security reports.

Office of Consumer Affairs & Business Regulation

Frequently Asked Questions

Better businesses. Smarter consumers.

Office of Consumer Affairs & Business Regulation

Q: What are the differences between this version of 201 CMR 17.00 and the version issued in February of 2009?

A: There are some important differences in the two versions. First, the most recent regulation issued in August of 2009 makes clear that the rule adopts a risk-based approach to information security, consistent with both the enabling legislation and applicable federal law, especially the FTC's Safeguards Rule. A risk-based approach is one that directs a business to establish a written security program that takes into account the particular business' size, scope of business, amount of resources, nature and quantity of data collected or stored, and the need for security. It differs from an approach that mandates every component of a program and requires its adoption regardless of size and the nature of the business and the amount of information that requires security. This clarification of the risk based approach is especially important to those small businesses that do not handle or store large amounts of personal information. Second, a number of specific provisions required to be included in a business's written information security program have been removed from the regulation and will be used as a form of guidance only. Third, the encryption requirement has been tailored to be technology neutral and technical feasibility has been applied to all computer security requirements. Fourth, the third party vendor requirements have been changed to be consistent with Federal law.

Office of Consumer Affairs & Business Regulation

Q: To whom does this regulation apply?

A: The regulation applies to those engaged in commerce. More specifically, the regulation applies to those who collect and retain personal information in connection with the provision of goods and services or for the purposes of employment. The regulation does not apply, however, to natural persons who are not in commerce.

Q: Does 201 CMR 17.00 apply to municipalities?

A: No. 201 CMR 17.01 specifically excludes from the definition of "person" any "agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof." Consequently, the regulation does not apply to municipalities.

Q: Must my information security program be in writing?

A: Yes, your information security program must be in writing. The scope and complexity of the document will vary depending on your resources, and the type of personal information you are storing or maintaining. But, everyone who owns or licenses personal information must have a written plan detailing the measures adopted to safeguard such information.

Q: What about the computer security requirements of 201 CMR 17.00?

A: All of the computer security provisions apply to a business if they are technically feasible. The standard of technical feasibility takes reasonableness into account. (See definition of "technically feasible" below.) The computer security provisions in 17.04 should be construed in accordance with the risk-based approach of the regulation.

Q: Does the regulation require encryption of portable devices?

A: Yes. The regulation requires encryption of portable devices where it is reasonable and technically feasible. The definition of encryption has been amended to make it technology neutral so that as encryption technology evolves and new standards are developed, this regulation will not impede the adoption of such new technologies.

Q: Do all portable devices have to be encrypted?

A: No. Only those portable devices that contain personal information of customers or employees and only where technically feasible. The "technical feasibility" language of the regulation is intended to recognize that at this period in the development of encryption technology, there is little, if any, generally accepted encryption technology for most portable devices, such as cell phones, blackberries, net books, iphones and similar devices. While it may not be possible to encrypt such portable devices, personal information should not be placed at risk in the use of such devices. There is, however, technology available to encrypt laptops.

Q: Must I encrypt my backup tapes?

A: You must encrypt backup tapes on a prospective basis. However, if you are going to transport a backup tape from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then you must do so prior to the transfer. If it is not technically feasible, then you should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, if you are transporting a large volume of sensitive personal information, you may want to consider using an armored vehicle with an appropriate number of guards.

Q: What does "technically feasible" mean?

A: "Technically feasible" means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

Q: Must I encrypt my email if it contains personal information?

A: If it is not technically feasible to do so, then no. However, you should implement best practices by not sending unencrypted personal information in an email. There are alternative methods to communicate personal information other through email, such as establishing a secure website that requires safeguards such as a username and password to conduct transactions involving personal information.

Q: Are there any steps that I am required to take in selecting a third party to store and maintain personal information that I own or license?

A: You are responsible for the selection and retention of a third-party service provider who is capable of properly safeguarding personal information. The third party service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the FTC's Safeguards Rule.

Q: I have a small business with ten employees. Besides my employee data, I do not store any other personal information. What are my obligations?

A: The regulation adopts a risk-based approach to information security. A risk-based approach is one that is designed to be flexible while directing businesses to establish a written security program that takes into account the particular business's size, scope of business, amount of resources and the need for security. For example, if you only have employee data with a small number of employees, you should lock your files in a storage cabinet and lock the door to that room. You should permit access to only those who require it for official duties. Conversely, if you have both employee and customer data containing personal information, then your security approach would be more stringent. If you have a large volume of customer data containing personal information, then your approach would be even *more stringent.*

Q: Except for swiping credit cards, I do not retain or store any of the personal information of my customers. What is my obligation with respect to 201 CMR 17.00?

A: If you use swipe technology only, and you do not have actual custody or control over the personal information, then you would not own or license personal information with respect to *that data, as long as you batch out such data in accordance with the Payment Card Industry (PCI) standards. However, if you have employees, see the previous question.*

Q: Does 201 CMR 17.00 set a maximum period of time in which I can hold onto/retain documents containing personal information?

A: No. That is a business decision you must make. However, as a good business practice, you should limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected and limit the time such information is retained to that reasonably necessary to accomplish such purpose. You should also limit access to those persons who are reasonably required to know such information.

Q: Do I have to do an inventory of all my paper and electronic records?

A: No, you do not have to inventory your records. However, you should perform a risk assessment and identify which of your records contain personal information so that you can handle and protect that information.

Q: How much employee training do I need to do?

A: There is no basic standard here. You will need to do enough training to ensure that the employees who will have access to personal information know what their obligations are regarding the protection of that information, as set forth in the regulation.

Q: What is a financial account?

A: A financial account is an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result. Examples of a financial account are: checking account, savings account, mutual fund account, annuity account, any kind of investment account, credit account or debit account.

Q: Does an insurance policy number qualify as a financial account number?

A: An insurance policy number qualifies as a financial account number if it grants access to a person's finances, or results in an increase of financial burden, or a misappropriation of monies, credit or other assets.

Q: I am an attorney. Do communications with clients already covered by the attorney-client privilege immunize me from complying with 201 CMR 17.00?

A: If you own or license personal information, you must comply with 201 CMR 17.00 regardless of privileged or confidential communications. You must take steps outlined in 201 CMR 17.00 to protect the personal information taking into account your size, scope, resources, and need for security.

Q: I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well?

A: Yes. If you own or license personal information about a resident of the Commonwealth, you must comply with 201 CMR 17.00, even if you already comply with HIPAA.

Office of Consumer Affairs & Business Regulation

Q: What is the extent of my "monitoring" obligation?

A: The level of monitoring necessary to ensure your information security program is providing protection from unauthorized access to, or use of, personal information, and effectively limiting risks will depend largely on the nature of your business, your business practices, and the amount of personal information you own or license. It will also depend on the form in which the information is kept and stored. Obviously, information stored as a paper record will demand different monitoring techniques from those applicable to electronically stored records. In the end, the monitoring that you put in place must be such that it is reasonably likely to reveal unauthorized access or use.

Q: Is everyone's level of compliance going to be judged by the same standard?

A: Both the statute and the regulations specify that security programs should take into account the size and scope of your business, the resources that you have available to you, the amount of data you store, and the need for confidentiality. This will be judged on a case by case basis.

Q: I password protect data when storing it on my laptop and when transmitting it wirelessly. Is that enough to satisfy the encryption requirement?

A: No. 201 CMR 17.00 makes clear that encryption must bring about a "*transformation* of data into a form in which meaning cannot be assigned" (emphasis added). This is to say that the data must be *altered* into an unreadable form. Password protection does not *alter* the condition of the data as required, and therefore would not satisfy the encryption standard.

Q: I am required by law to contract with a specific third party service provider not of my choosing. Will I still be expected to perform due diligence in the selection and retention of that specific third party service provider?

A: Where state or federal law or regulation requires the use of a specific third party service provider, then the obligation to select and retain would effectively be met.