2012 Data Privacy Report

and Report on Remedial Steps in Aftermath of Significant Breaches

Deval Patrick
Governor

Office of Consumer Affairs & Business Regulation
Better businesses. Smarter consumers.

Barbara Anthony
Undersecretary

DATA BREACH ANNUAL REPORT

The Commonwealth's Data Breach Security Law, Mass. General Law, Chapter 93H, has been in effect since October 31, 2007. The law requires businesses and others that own or license personal information of residents of Massachusetts to notify the Office of Consumer Affairs and Business Regulation and the Office of Attorney General when they know or have reason to know of a breach of security. They must also provide notice if they know or have reason to know that the personal information of a Massachusetts resident was acquired or used by an unauthorized person, or used for an unauthorized purpose. In addition to providing notice to government agencies, businesses or individuals that store or maintain personal information must notify the owner or licensor of the information if they know or have reason to know of such a breach, acquisition or use.

What is personal information? Chapter 93H, §1(a) defines "personal information" as: "a resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: Social Security number; driver's license number or state-issued identification card number; or 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; provided, however, that 'personal information' shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

On March 1, 2010, the Data Security Regulations, 201 CMR 17.00, promulgated by the Office of Consumer Affairs and Business Regulation went into effect. The regulations implement the provisions of Chapter 93H by establishing the standards to be met by persons or businesses that own or license personal information of residents of the Commonwealth and the minimum requirements for which they are responsible in protecting that personal information, stored in electronic and paper format.

Under the regulations, persons or businesses owning or licensing personal information of residents of the Commonwealth must develop, implement and maintain a comprehensive written information security program ("WISP"), containing administrative, technical and physical safeguards that are appropriate to the: size, scope and type of business of the person or business obligated to safeguard that personal information; amount of resources available to that person; amount of stored data; and need for security and confidentiality of both consumer and employee information.

One of the most critical features of the Massachusetts law is the requirement that personal information be encrypted if it is transmitted over public networks, the internet or carried on portable devices such as laptops or compact discs. As defined by the regulation, "encryption" is technologically neutral, and requires the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

The regulations also provide that persons owning or licensing personal information who utilize third party service providers must oversee the service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate security measures for personal information. These measures must be consistent with Massachusetts regulations and, on or before March 1, 2012, those persons must require the third party service providers by contract to implement and maintain such appropriate security measures and safeguards.

During 2012, the Office of Consumer Affairs and Business Regulation received 1,143 reports of incidents of data breaches from businesses and entities in conjunction with their mandated reporting. Although most of

these notifications did not distinguish between security breaches involving encrypted or unencrypted personal information, the data contained in these reports suggests that the personal information compromised in these breaches was not encrypted. While businesses are not required to include in their notifications that the particular data breach involved encrypted or unencrypted information, that element of the nature of the breach is substantial in reviewing the success of encryption and furthering the protection of personal information.

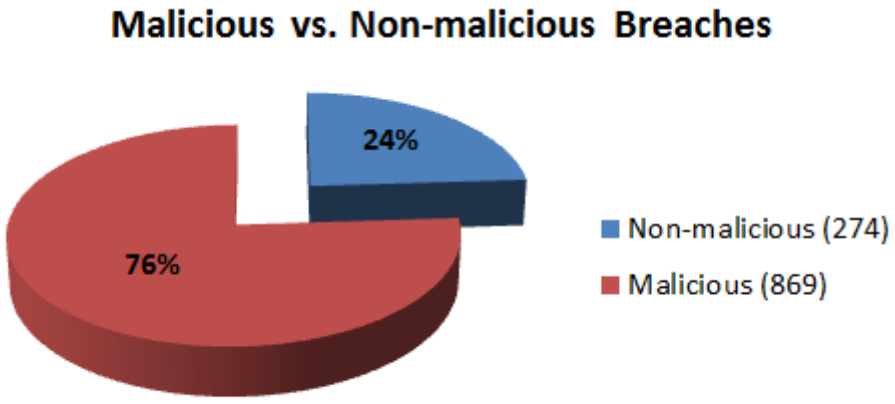
According to the 2012 notifications, the total number of Massachusetts residents affected by data breaches was 340,462. This is significant because it is the lowest number of Massachusetts residents reported to the Office as being affected by data breaches in each full year since the law took effect.

During 2012, a total of 1,143 data breach notifications were received by the Office of Consumer Affairs, affecting over 340,000 Massachusetts residents.

As in previous years, the reports of data breach incidents to the Office included both criminal or "malicious" acts and unintentional, "non-malicious" acts. Malicious breaches describe those that are intentional, unauthorized intrusions into any databases of personally identifiable information. These can range from outside intrusions into electronic databases, often referred to as "hacking" computer systems, and the use of computer programs designed to access personal information without authorizations by placing "malware" in the system to divert personal information to an unauthorized location, to intentionally opening or breaking into a file cabinet and accessing files with personal information contained therein. A malicious breach can also include the intentional acts of current or former employees, whose access privileges were not monitored appropriately or terminated properly in a timely manner.

MALICIOUS VS. NON-MALICIOUS BREACHES

Based upon the 1,143 data breach reports in 2012, 869 or 76 % were "malicious" or intentional data breaches, affecting 225,525 residents of the Commonwealth. Many of these incidents were reported as being caused by deliberate hacking, criminal theft, and unauthorized access by a current or former employee according to the businesses. The Commonwealth's regulations emphasize the importance of preventing terminated employees from accessing records that contain personal information. To the extent that one employee may know another employee's password or access codes, businesses must ensure that such codes are also regularly changed, and restricted or changed upon the resignation or termination of an employee.



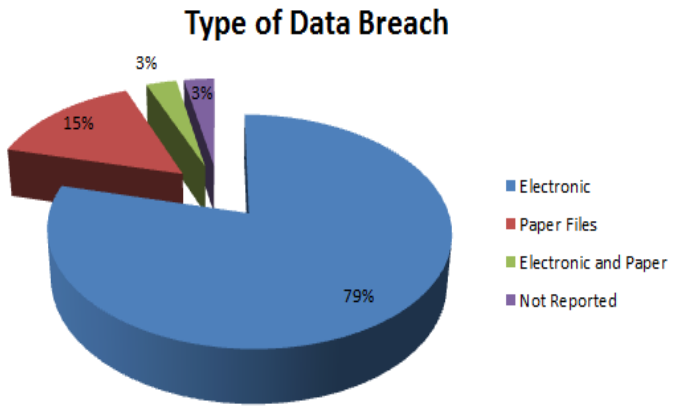
Notably, in 2012, the number of unintentional, non-malicious breaches was 274 or 24% of the total reported, and these affected approximately 114,937 Massachusetts residents. These breaches are deemed "non-malicious" because the information received in the reports to our Office suggests that the breach resulted from negligence attributable to the business or its employees. Non-malicious breaches are certainly the most preventable breaches. As reported in 2012, these data breaches were caused by

employee mistakes or organizational lapses that, in many instances, were avoidable. Many of the reported breaches could have been reduced or negated entirely if the businesses had implemented stricter internal controls, combined with proper training regimens for their employees. With regular training, employees can be educated significantly on the importance of the protection of personal information, the reinforcement of privacy policies, quality control, follow up, and protocols for proper supervision. Data breaches that are entirely preventable continue to include employee mistakes involving wrong address, wrong envelope, incorrect email address or recipient, attaching wrong document, wrong fax number, and losing or misplacing a portable device. Certainly, regular trainings and strict supervision of employees emphasizing their responsibility and obligation to protect personal information would have reduced the number of data breaches.

Businesses and organizations, large and small, are not only required to have a WISP in place under the law, but they must also ensure that their employees and third party vendors and processors are appropriately aware of, educated and trained in the handling and management of personal information and the significance of the protection of that information.

ELECTRONIC BREACHES DOMINATE REPORT RESULTS

In 2012, the overwhelming majority of data breach incidents involved electronic records. There were 902 instances or 79% of the total number of reported breaches that involved personal information in electronic form. Data security breaches of paper files, including fax, email and snail mail, accounted for 175 of the 1,143 reported or 15%, while 30 breaches or 2% of the total involved both electronic and paper, and another 36 or 3% were not defined as electronic or paper records by the business entity or person making the report. Both paper and electronic files can be protected by limiting access to them and destroying them when no long needed. Electronic devices present unique challenges for transferring and disposing of personal information and businesses are encouraged to be active in keeping abreast of trends and regularly reviewing and updating their security measures especially with respect to portable devices to prevent compromised systems.



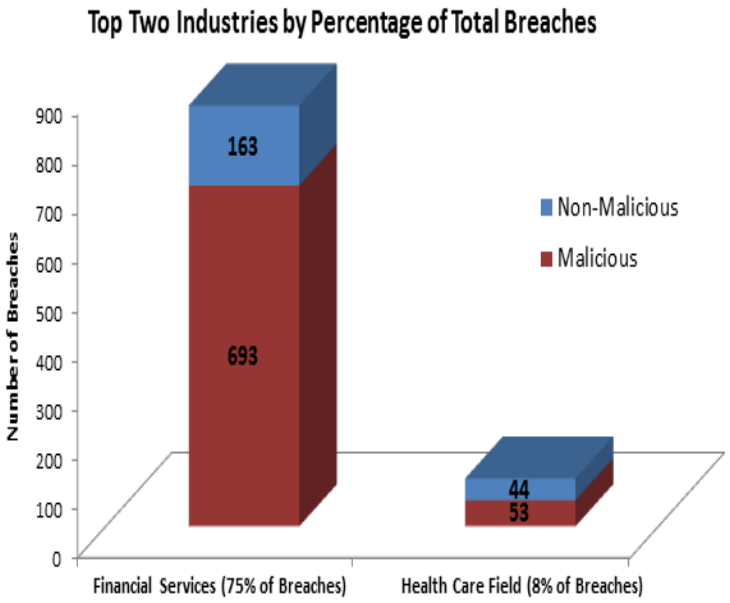
MOST AFFECTED INDUSTRIES

According to the 2012 reports submitted to the Office, the data security breaches affecting the largest number of residents and occurring with the greatest frequency involved compromised credit or debit card account numbers. Of the 1,143 data breach notifications that the Office received in 2012, 725 or 63% included the breach of credit or debit card account information. Although banks and credit card companies are responsible for reporting the data breaches, they are often not the cause of the security breaches. Most breaches reported by banks occur at payment processing centers and retailer establishments. Because banks own the compromised personal information connected to the cards, they must report the breach. In many instances, the breach occurred with a third party processor, at a domestic, foreign or online retail location where the terminal or PIN pad was hacked or unauthorized use occurred. As the protected information is generally financial in nature, not surprisingly, in 2012 as in previous years, the largest number of data

In 2012, 725 or 63% of breaches included residents' credit or debit card information.

breaches impacting the largest number of Massachusetts residents was reported by the financial services industry. That business sector accounted for 856 data breaches or 75% affecting 186,025 residents of the Commonwealth. Of these 856 breaches, 693 or 81% were categorized by the Office of Consumer Affairs and Business Regulation as malicious and 163 or 19% deemed non-malicious.

Following the financial services industry in numbers of data breaches was the health care field with 97 reported data breaches or 8% in 2012, of which the Office determined from reports that 53 incidents were malicious, and 44 were non-malicious, affecting a total of 22,355 residents of the Commonwealth.



TRENDS AND PATTERNS

In some respects, the reports received by our Office in notifications of data security breach incidents for 2012 were encouraging as compared to 2011. For example, the total number of Massachusetts residents reportedly affected by data security breaches decreased 68% in 2012 to 340,462 from 1,090,330 in 2011.

It seems likely that fewer residents were affected in these data breaches because many of the 2012 notifications provided to our Office indicated that the data breaches were smaller and more limited, affecting smaller numbers of Massachusetts residents. Perhaps more businesses are actively engaged in employing tactics and procedures to protect their customers' personal information than in years past. Unfortunately, however, even though Chapter 93H has been in effect for over five years and the regulations for more than three years, the evidence contained in the 2012 notifications also suggests that none of the personal information compromised in these data security breaches was encrypted. While there were 1,533 Massachusetts residents protected through encryption in malicious and non-malicious breaches reported in 2011, in contrast, it appears that there were no Massachusetts residents protected by encryption in any of the reported incidents of data security breaches in 2012.

Total residents affected in 2011: 1,090,330

Total residents affected in 2012: 340,462

In fact, the largest data breach in 2012, affecting 73,240 Massachusetts residents and accounting for almost 22% of the residents affected by data security breaches in the Commonwealth that year, was reported by TD Bank, N.A. According to the Office of the Massachusetts Attorney General, the bank notified them that two unencrypted backup tapes containing the personal information of bank customers were lost or misplaced while en route to an offsite bank location. While TD Bank evidently learned of the breach in March 2012, it did not report the incident to its affected customers in multiple states including Massachusetts, the Office or the Attorney General until October, a period of more than five months. The breach is noteworthy because it highlights the need for stricter protocols by businesses to ensure that their employees and third party contractors are educated and trained properly in securing and protecting the personal information of their customers and emphasizes the importance of encryption as a necessary component of any business's written information data security plan.

One of the troubling aspects of data security breaches that continued in 2012 from 2011 was the effect of lost or stolen mobile devices containing personal information that appears to have been unencrypted on residents of the Commonwealth. Our Office received 40 separate reports of incidents concerning mobile devices where personal information was compromised. These breaches involving mobile devices, including discs, laptops, iPads, thumb and flash drives, accounted for 26% of the total number of Massachusetts residents affected in 2012 or 89,755. In comparison, the number of reported lost, misplaced or stolen devices in 2011 was 63; and the number of residents affected by those data breach incidents was significantly less than 2012 at approximately 28,000 or only 2.5% of the total. But for the single data breach incident involving TD Bank in 2012 affecting 73,000 Massachusetts residents, the compromised mobile devices would not have caused as much of an impact, only affecting 5% of the total for 2012.

REPORT ON REMEDIAL STEPS IN THE AFTERMATH OF SIGNIFICANT BREACHES

Businesses Take Privacy and Data Security Seriously

Massachusetts law requires businesses or agencies that own or license personal information of residents of the Commonwealth to provide notice to the Attorney General and Office of Consumer Affairs and Business Regulation when they have suffered a data breach. Specifically, Chapter 93H §3(b)of Mass. General Laws states: "The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident."

In an effort to ascertain the internal response of businesses to their reported data breaches, the Office of Consumer Affairs and Business Regulation gathered additional relevant information through a follow up inquiry conducted in mid-2012. The Office selected 19 organizations that had reported data breaches affecting over 5,000 Massachusetts residents in the time period from January 2010, through April 2012 and sent letters to these businesses on June 25, 2012, requesting specific information about the data breaches and the actions taken in response. The Office inquired about the company's WISP and whether it was in place at the time of the data breach. If it was not clear from the entity's initial report whether the personal information that was breached had been encrypted, the Office also asked for the procedures that the organization instituted since the breach relating to data encryption. Additionally, the Office sought a copy of a sample contract provision that the company currently utilizes with its third party providers to protect the personally identifiable information of Massachusetts residents, as well as detailed information relative to employee training and awareness programs that the organization has instituted since the reported breach.

Not only did our Office receive responses from all 19 businesses, but more impressively, most of the organizations provided us with more detailed information regarding the specific breach, the steps undertaken to respond appropriately, and the measures instituted to prevent such a breach from occurring again in the future. The businesses were cooperative and helpful in providing us with a more detailed view of the particular breach and their individual response.

It was evident from the level of detail of the organizations' collective response to our Office that businesses, reacting to their own reported breach, took the issue of data security and the protection of personal information

seriously. Overall, these organizations reported that they reviewed and investigated the particular breach and determined its internal or external cause, whether malicious or unintentional, the size and severity of the breach, as well as remedial steps that should be taken preemptively as a deterrent to a future recurrence. Many reported that they examined the absence of any effective data security protocol internally and actively engaged in a review and revision to establish and implement new procedures preventively and address the individual breach. Nearly all of the businesses submitted, as requested, some form of a WISP and third party contract language mandating that party's compliance with the Massachusetts data security laws. Fewer organizations responded with specific information on their employee awareness training relative to data security. However, a variety of other documents submitted to our Office by organizations demonstrated their efforts at tightening or revising their data security protections. These documents included a Computer Use Policy, a Background Check Policy, a receipt for the destruction of physical servers containing personal information, and even a former WISP for comparison purposes. Other documents submitted were specific to the particular breach that had occurred.

We contacted businesses that had breaches affecting over 5,000 Massachusetts residents between 2010 and 2012. All 19 businesses responded with information about specific steps they had taken after being breached.

Below are some specific examples of how Businesses responded to our request for more information.

SOUTH SHORE HOSPITAL

The largest data security breach affecting the most Massachusetts residents among the 19 organizations was reported by South Shore Hospital in Weymouth, Massachusetts. That breach, reported to our Office on July 17, 2010, involved missing backup data tapes, which affected the personal information of approximately 800,000 Massachusetts residents. The Hospital notified us that in February 2010 it had shipped three boxes containing 473 unencrypted back-up computer tapes with Massachusetts residents' personal information and protected health information off-site to be erased and had contracted with a third party vendor to carry out this project. According to the Hospital's report, it learned in June of 2010, that two of the three boxes were missing and had not arrived at their destination. The boxes were never found, but there was no evidence of unauthorized use of any of the personal information contained in the tapes.

Following an investigation by the Massachusetts Attorney General's Office, the Hospital entered into a consent judgment to resolve the allegations of violations of state and federal law. In its press release of May 24, 2012, the Attorney General announced that the personal information compromised in the data breach included "individual's names, Social Security numbers, financial account numbers and medical diagnoses." The Attorney General also reported that as part of the consent judgment, the Hospital had agreed to pay a significant fine, undergo a review and audit of its privacy procedures and take a number of steps towards correcting and revising its policies towards protecting personal information. When the Hospital filed its additional report to our Office on July 20, 2012, the Hospital indicated that it had revised its WISP with new procedures relating to the encryption of data to be transmitted wirelessly or held on portable electronic devices and implemented a comprehensive training regimen for its workforce upon hire and conducted during Hospital

South Shore Hospital responded to a breach affecting approximately 800,000 Massachusetts residents by undergoing a security audit and updating its security policies.

orientation. The Hospital now requires that its employees complete mandatory education modules on an annual basis, with testing on privacy and security competencies. Although South Shore Hospital informed us in the July 20, 2012 letter that it had a WISP in place at the time of the breach, it revised that WISP after the data loss. In its July report, the Hospital provided the Office with the updated WISP, the third party contract provision and its "Workstation and Computing Device Acceptable Use Policy" for its workforce members, including employees, vendors, contractors, volunteers or business associates who have access to the hospital's computing network or resources.

SONY NETWORK ENTERTAINMENT

Sony Network Entertainment suffered an illegal and unauthorized data security breach between April 16 and 17, 2011 in their PlayStation Network and Qriocity platform and notified the Office of Consumer Affairs and Business Regulation on May 2, 2011.

Sony reported that the intrusion affected 470,000 Massachusetts residents and compromised personal information stored in electronic form including customer names, addresses, e-mail addresses, billing addresses, birthdates, passwords, login, and PlayStation Network online IDs.

The organization, in response to the enormity of the breach and our request for additional information, notified our Office on August 9, 2012 that it had implemented a number of security policies subsequent to the intrusion. Specifically, Sony reported that it expedited the movement of its data center from its current location to a more secure facility. The company had planned the move, but hastened the timing of it following the discovery of the data breach. Sony also reported that it had, both before and after the intrusion, been committed to instituting robust security capabilities. In furtherance of this commitment, Sony reported that it implemented additional automated monitoring of its software to defend against attacks, enhanced its levels of data protection and encryption with additional firewalls, and augmented its capabilities to detect software intrusions, unauthorized access and unusual activity patterns within the network. Sony Network supplemented their existing security personnel by creating a new management level position of Chief Information Security Officer, directly reporting to the Chief Information Security Officer of Sony Corporation. According to Sony, the company had instituted a practice of administering security awareness training to all employees before the breach incident and, as of April 2012, all employees had completed this training and were required to complete a further training by the end of 2012. As requested by our Office, Sony responded cooperatively by providing us with a copy of its WISP, its third party contract language, and its security training plan document together with its other security policies and procedures.

After being breached in 2011, Sony implemented additional attack monitoring, enhanced its network security, and created a Chief Information Security executive to oversee company data policies.

ECMC-EDUCATIONAL CREDIT MANAGEMENT CORPORATION

Shortly after our Data Security Regulations went into effect on March 1, 2010, ECMC Group of Oakdale, Minnesota, reported to the Office on March 29, 2010, and April 9, 2010, a theft of two safes from their premises. According to ECMC, the safes contained DVDs that included individual borrower names, addresses and Social Security numbers, and in some instances, driver's license numbers. ECMC estimated that the

breach affected approximately 65,832 Massachusetts residents and included with its report a copy of a press release by the Minnesota Department of Public Safety indicating the recovery of the safes and digital media within 48 hours of the theft. The department reported that it did not believe the information had been accessed or compromised.

In response to our request for additional information, ECMC informed us that it undertook a number of measures to address the malicious data breach theft. For example, ECMC reported that it had commissioned a risk assessment audit by a third party auditor, the findings of which were beneficial in providing direction to the company in formulating a plan to revise its security to protect personal information. Specifically, ECMC developed strategies for increasing its physical security and its information data security. The organization placed guards in strategic locations throughout its facility, installing cameras and expanding the employee ID badge tracking system across all locations for employees, visitors and invitees. Some of its related tactical initiatives included cable locks for laptop and desktop computers, facility alarm systems to cover all entry and exit points and ongoing security training, as well as incident response. It restricted the access of employees to information deemed sensitive, disabled media removal on employee workstations, revised employee data security training and implemented enhanced software protection, including establishing enhanced monitoring procedures for electronic and physical access. It enhanced its encryption practices to include all mobile devices, desktops and laptops. ECMC also provided us with its WISP, employee training program, a Strategic Security Plan and a sample of its third party contract language.

ECMC responded to its 2010 breach by commissioning a third party risk assessment and implementing new physical and information.

AARON'S INC.

On October 19, 2011, Aaron's Inc. of Kennesaw, Georgia, reported to us that it had suffered a data breach when a franchisee store in California was burglarized and an assortment of goods, including computers, was stolen. One of the computers was used in the daily operations of the store and contained a file with personal information, possibly including the names and Social Security numbers of individual customers. Aaron's reported the theft to the local law enforcement authorities and conducted an internal investigation of the crime. From their investigation, Aaron's informed our Office that they estimated the personal information of approximately 17,043 Massachusetts residents was acquired but not accessed. The company further advised us that it offered credit monitoring services and call center support to the residents whose personal information had been compromised. Following the June 2012 request, the only documentation that Aaron's provided to our Office was its third party servicer contract language. Aaron's reported that it took the data breach very seriously and was in the process of reviewing its privacy and security practices and addressing relevant issues identified in that review. However, neither the company's WISP nor any information relating to the implementation of employee training and awareness programs was included in its response.

Aaron's provided credit monitoring services to residents whose information may have been compromised.

BELMONT SAVINGS BANK

On May 31, 2011, Belmont Savings Bank reported a data security breach to our Office. The Bank informed us that it suffered the breach when a backup server tape containing customer account data was inadvertently discarded, affecting the personal information of approximately 13,380 Massachusetts residents. After

reviewing their bank surveillance tapes, Belmont Savings determined that the tape had fallen into the trash and been incinerated by its disposal contractor.

In contrast to the limited response we received from Aaron's, Belmont Savings Bank reported extensive steps that it undertook to address the lapse. First, the bank eliminated from its protocol the use of physical backup tapes altogether. According to Belmont Savings, all backups are now completed electronically through a secure encryption connection to an external vendor. The Bank revised its WISP and undertook the destruction of all of its stale electronic data. It also established a stringent policy concerning the disposition of electronic customer information. Additionally, the Bank provided an information security clause for third parties to detail their contract requirements relative to protecting personal information of all Bank customers, and included a section of a current contract demonstrating the vendor's responsibility. Finally, the Bank advised us that it implemented additional mandatory employee privacy training on data security awareness. Belmont Savings submitted to us a copy of its WISP, entitled "Electronic Information Security Policy," its "Privacy Policy - Policy of Safeguarding Customer Information" which includes an incident response policy in the event of a breach, Annual Privacy notice, and its compliance training for employees known as "Information Security and Red Flags Online Training" with checklist and calendar.

Belmont Savings Bank began encrypting and storing backups online after a backup tape was accidentally discarded.

MICHAELS STORES, INC.

On May 31, 2011, our Office received a notification from Michaels Stores, Inc. that they had suffered a data security breach affecting the personal information of approximately 41,000 Massachusetts residents. According to Michaels' updated report on August 28, 2012, they had retained, following the breach, an outside consultant to perform a forensic analysis. The analysis indicated that unauthorized individuals removed certain point of sale personal electronic devices from Michaels store locations, retrofitted the devices with an additional memory chip and transmitter, and reinstalled the devices in Michaels stores to download the debit card and accompanying PIN number through the Bluetooth transmitter from outside the store. Michaels reported that the stolen data was unencrypted because it was obtained before it entered the Michaels point of sale system.

In its August 2012 report, the business advised that it undertook a number of steps to address and respond to the breach, reporting that it had worked with the U.S. Secret Service to find the perpetrators of the crime. It also conducted an independent third party review of its data security system with the goal of making revisions and adding protections to prevent such an incident from occurring in the future. Michaels established an internal Information Security Advisory Board to provide updates and track the progress of its security plan. Additionally, it enhanced its store level security in the physical sense by: installing new tamper-resistant point of sale systems with restricted access to point of sale by management personnel; restricting third party access to the point of sale system; and mandating manager training to provide for detailed inspection of point of sale systems. As of August 28, 2012, Michaels was working closely with IBM to develop software that would make it impossible for a fraudulent perpetrator to remove, reconfigure and replace the point of sale personal electronic device at the store register. This software was in testing as of August 2012 and Michaels reported that it planned to ensure that it was

Michaels worked with the U.S. Secret Service to find the perpetrators of its 2011 security breach. Michaels then consulted with IBM to develop fraud-proof point of sales systems for its stores to prevent similar breaches.

installed in all its stores when finalized. Michaels submitted their previous WISP, a revised WISP and a sample contract provision which Michaels currently uses with their third party vendors governing confidential and personally identifiable information. The company notified the Office that it had revised its WISP to include enhanced and expanded provisions pertaining to all of the above upgrades.

CONCLUSIONS

The businesses contacted by the Office of Consumer Affairs in an effort to gather additional information concerning data breaches affecting more than 5,000 Massachusetts residents were very responsive. In almost every instance, the organization, following discovery of the data breach, undertook a review of its existing data privacy policy, and consequently implemented both internal physical security initiatives as well as information security measures to curtail the loss and reduce the risk of future incidents. Some of the organizations retained outside vendors to conduct an audit and risk analysis with proposed revisions; others rewrote their WISP and incorporated additional physical and data security enhancements, while others focused on strategic planning and completely revised their privacy policies. Most of the businesses or organizations reported that they incorporated increased employee training into their regimen, while updating their workforce computer policies.

The Office of Consumer Affairs and Business Regulation was encouraged by the responsiveness of these businesses to undertake necessary steps to strengthen the security of customer and employee personal information. Our Office is available to provide trainings and seminars to businesses that are interested in learning more about our state's data security laws and regulations. For further information, please contact Joanne F. Campo, Deputy General Counsel at 617-973-8708, or Julian W. Smith, Consumer Research and Programs Manager at 617-973-8741.