In the world of data privacy and security, the year 2013 concluded dramatically with the news that Target had suffered a massive data breach affecting tens of millions of consumers across the United States during the prime holiday shopping season. Here in the Commonwealth of Massachusetts, the Office of Consumer Affairs and Business Regulation learned by written notice that approximately 947,000 Massachusetts residents were affected by the Target breach. While the magnitude of the breach has resulted in an ongoing investigation by the Department of Justice, Target did report that their systems were hacked and over 40 million debit and credit card numbers were stolen from Target customers. Within a few weeks of that announcement in December, Target further reported that the fraudsters had also lifted the personal information of an additional 70 million customers in the attack, including names, home addresses, email addresses and telephone numbers, with some overlap between the two impacted customer groups. The widespread impact of the Target breach in late 2013 was felt considerably in the Commonwealth as the number of Massachusetts residents impacted by data breach incidents rose significantly last year with that event.

Number of Reported Data Breaches Increased from 2012

1,821 1,163,643

Total reported breaches in 2013  Total Massachusetts residents affected

During 2012, the Office of Consumer Affairs and Business Regulation received 1,143 notifications of data breach incidents. In 2013, that number increased by 59% over 2012 as the Office received 1,821 reports of data breaches affecting 1,163,643 residents of the Commonwealth, which includes the approximately 947,000 Massachusetts residents impacted by the Target breach in December. Interestingly, without Target, the remaining number of Massachusetts residents whose personal information was affected by data breaches according to the Office notifications was 216,642, which is 36% fewer than 2012 when 340,462 residents were impacted by data breaches. With the exception of Target, it appears that although the number of reported breaches increased significantly from 2012 to 2013, there were smaller numbers of Massachusetts residents impacted by many of the reported data breaches. This is especially encouraging as Massachusetts has one of the most stringent and protective laws pertaining to data security in the nation.

History, Law and Regulations

The Data Security Law, Chapter 93H of the Massachusetts General Laws which took effect in 2007, requires businesses and entities that own, license or maintain personal information of residents of the Commonwealth to notify the Office of Consumer Affairs and Business Regulation and the Office of the Attorney General when they know or have reason to know of a breach of security, or if the
personal information of a Massachusetts resident was acquired or used by an unauthorized person, or used for an unauthorized purpose. Those businesses that store or maintain such personal information must also notify the owner or licensor of the information 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.”

In the notification law, Chapter 93H, the Office of Consumer Affairs and Business Regulation was tasked with the authority to promulgate the data security regulations in support of the statute and more specifically, to provide businesses with information pertaining to their obligations under the law.

The regulations, 201 CMR 17.00, written and promulgated by the Office of Consumer Affairs and Business Regulation, took effect in March 2010. They set forth detailed provisions and requirements for businesses in creating effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth that they own, license, maintain or possess. The three major components of the regulations are the Written Information Security Program, encryption and the exercise of due diligence with third party contracts.

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 or “WISP” that contains administrative, technical and physical safeguards appropriate to the: size, scope and type of business they have; extent of resources available to the person or business; amount of stored data; and need for security and confidentiality of both customer and employee information. An important requirement for businesses is that they conduct regular monitoring of their WISP to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and they review their program annually or sooner if there are changes in their business practices. It is incumbent upon each business under the regulations to ensure that their employees who have access to personal information are trained as often as is necessary so that they comprehend their responsibilities and obligations in the protection of that information. The WISP must include provisions regarding employee training and compliance as well as policies and procedures for the storage, access and transport of personal information. If a data breach occurs, the business is required under the WISP to document their response to such a breach.
Additionally, the regulations require encryption of data that is transmitted across public networks, or transmitted wirelessly, and if it is stored on laptops or other portable devices. Since the regulations were written prospectively after careful consideration of the needs and comments of businesses that provided input at the time of their proposal, the word “encryption” was defined in a technologically neutral way to allow flexibility for continually changing standards for encryption and technological innovation. Encryption, therefore, is defined in the regulation as “the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.”

Businesses that employ the services of third party vendors are required by law, as set forth in the regulations, to conduct due diligence and take reasonable steps in selecting those vendors, to ensure that they are capable of utilizing and maintaining appropriate security measures in protecting personal information for or on behalf of the business. There must be included in the contract a provision that binds the third party vendor to compliance with the Massachusetts data security law.

The regulations, while strict, do adopt a risk-based approach to assessing the protection and security of personal information. They were designed and written to be flexible in mandating that businesses create and implement a WISP, so that entities could take into account their individual size, scope of business, type and extent of resources, and their particular need for security. Ultimately, it is important that businesses develop and promote a culture of security within their organization, regardless of size, and demonstrate a commitment to protecting the personal information that they own, license or possess to reduce the risk of an information breach.

Does Your Business Have a WISP?

Persons or businesses owning or licensing personal information must develop, implement and maintain a comprehensive Written Information Security Program or “WISP.”

Persons or businesses owning or licensing personal information must develop, implement and maintain a comprehensive Written Information Security Program or “WISP.”
**Electronic Breaches**

Last year, as in the years since the data breach law took effect in late 2007, the overwhelming majority of data breach incidents involved electronic records. Of the 1,821 total breaches reported to the Office in 2013, 1,606 or 88% related to compromised personal information in electronic form. The remaining 12% was broken down as follows: 176 data security breaches of personal information held in paper format, such as hard copies of documents, faxes, emails and regular postal mail accounted for 10%, while 18 breaches or 1% involved both electronic and paper, and another 21 or 1% were undefined by the business entity.

**Affected Industries**

In 2013, the financial services industry reflected significant data breach activity and reported 1,551 data breaches accounting for 85% of the total reported for the year to the Office. This business sector provides economic services to consumers and businesses and encompasses a wide range of financial institutions that manage money, including banks, credit unions, insurance companies, brokerage firms, consumer finance companies, and investment companies.

There were 90,043 residents affected by financial services data breaches and approximately 75% of these 1,551 notifications were deemed intentional or malicious based upon the information provided by the businesses to the Office in their written notifications. Banks and credit unions, while responsible for reporting the data breach incidents because of their ownership of the personal information breached (credit and debit cards), are not generally the root cause of the information security breach.

The data received by the Office for 2013 again demonstrates that these breaches largely occur at payment processing centers and retail establishments. In fact, most of the breach incidents reported by
banks and credit unions occurring at payment processing centers and retail establishments are connected to a third party processor, at a domestic, foreign or online retail location where the terminal or PIN pad was hacked or an unauthorized use took place.

Since the data protected by the financial services industry, including Social Security numbers and financial account numbers, is by its very nature, financial and linked to money held in those accounts, it is a high value target for fraudsters. Not surprisingly, of the 1,821 data breach notifications received by the Office in 2013, 1,387 or 76% included the breach of credit or debit card account information and most of these reportedly occurred within the industries of banks and credit unions.

Following financial services last year was the health care field, which reportedly experienced 88 data breach incidents or 5% of the total, affecting 6,371 residents of the Commonwealth. In comparison to 2012 when that industry notified the Office of 97 breaches or 8% of the total and ranked second in industry breaches, the sector suffered fewer data breaches in 2013. Based upon the notifications, 26 of the 88 or 30% were deemed to be malicious or intentional data breaches.

In 2013, an industry experiencing data breaches that affected a large number of residents was the technology industry, which reported 16 data breaches affecting 52,227 residents of the Commonwealth. These statistics are very similar to those reported for that industry in 2012.

**Personal Information Breached by Industry**

![Graph showing personal information breached by industry]

**Retail services experienced 24 reported data breaches last year, including the Target breach which affected approximately 947,000 Massachusetts residents.**
Retail services experienced only 24 data breaches last year, but as that number included Target, almost one million Massachusetts residents-954,212 were affected. Without the massive Target breach, approximately 7,200 Massachusetts residents would have been impacted by retail breaches in 2013. Of the 24 retail industry breaches, all but two were determined by the reports to be electronic. The Target data breach is remarkable because it highlights the enormity of such an incident on a nationwide retailer’s customer base across the United States. It serves as a sobering reminder to businesses to continue to be watchful and vigilant as guardians of customers’ personal information.

Interestingly, in 2013, the education sector experienced a significant change from past years. Previously it had been an industry that had drawn little attention and remained unremarkable in data breach occurrences. According to the 20 reports of data breach incidents received in 2013 from educational institutions, however, the personal information of 31,870 residents of the Commonwealth was compromised last year. This is a 611% increase from 2012 when the number of Massachusetts residents affected by breaches in this sector was 5,208. In 2013, all 20 were electronic breaches and 17 of the 20 were determined to be malicious, based on the incident reports. Fifteen of the 20 related to personal information that included Social Security numbers. This upsurge in data breaches within the education sector could be indicative of a trend in which cybercriminals and hackers are seeking a portal in this industry through which to steal personal information. Fraudsters could be enticed by the vast amounts of personal information held in the computer security systems of colleges and universities generally, as they may retain the personal information, including Social Security numbers, of current and former students, alumni and others for many purposes, including enrollment and financial aid. Certainly the escalation of data breach incidents observed in the education industry highlights the importance that these institutions must place on their protection of personal information to avert future breaches.

**Malicious v. Non-Malicious Breaches**

Based upon the information contained in notifications the Office of Consumer Affairs and Business Regulation received from reporting entities 1,532 or 84% of the data breaches were deliberate, affecting approximately 1,123,735 residents of the Commonwealth. These were deemed to be “malicious” because the incidents surrounding the breaches were of an intentional nature. Causes of the data breaches included theft of documents, computers and portable devices, intentional misuses by employees, deliberate hacking, the placement of a malicious code or software known as “malcode” or “malware” in the business’s computer system to divert personal information to another location for an unauthorized use and criminal theft or activity. The aim, of course, of the malicious, intentional or criminal behavior is identity theft, fraud and financial gain on the part of the fraudsters and hackers.
As malicious behavior becomes more sophisticated with respect to diverting personal information, the necessity on the part of businesses to increase their vigilance and promote an organizational culture of awareness and security in the guardianship of personal information is more pronounced.

**Although only 38 mobile devices were lost or stolen, none of the devices were encrypted as the regulations require.**

In 2013, only 288 or 16% of the 1,821 data breach notifications received by the Office were categorized as non-malicious, unintentional or accidental in nature. These were determined to be non-malicious because the information related in the reports to the Office of Consumer Affairs and Business Regulation suggested that the breach resulted from an accidental or otherwise unintentional act committed by the business, its employee(s) or a third party vendor. There are many different ways in which personal information retained, held or maintained by a business or entity can be compromised resulting in a data breach under Massachusetts law and triggering the statutory notification.

For example, in 2013, the Office continued to receive reports from businesses detailing employee mistakes that caused a data security breach. There were, as in previous years, incidents described as: labeling the wrong address on an envelope or package; inadvertently putting documents containing personal information in the wrong envelope; mailing envelopes with open windows that display and expose personal information, including Social Security numbers and tax identification numbers in the exposed window; using the wrong email address in sending a client’s or customer’s personal information to a recipient; accidentally including a copy of a tax return with the Social Security number of another residential loan applicant to another mortgage applicant; attaching a wrong document; using an incorrect fax number; leaving paper documents with the personal information of clients, customers or patients in a motor vehicle; and losing or misplacing a laptop or portable device containing personal information.

**Mobile Devices**

A positive development observed in 2013 is that fewer reports of data breach incidents concerning lost, misplaced or stolen mobile devices were submitted than in any year since the law went into effect in 2007. There were only 38 reported for 2013. In 2012, there were 40 data breach incidents involving lost, misplaced or stolen mobile devices;
in 2011, there were 63; in 2010, there were 72; in 2009 there were 73; and in 2008 there were 147 reported.

As reported in 2013, these 38 breaches involved portable devices such as discs, laptops, thumb and flash drives, backup tapes, and a handheld scanner and impacted 8,140 Massachusetts residents or 0.7% of the total residents affected. In comparison to 2012, when the number of Massachusetts residents affected by lost, misplaced or stolen portable devices was reported to our Office as totaling 89,755, the decrease of more than 90% is certainly significant. Perhaps the trend downward of fewer data breaches from lost, misplaced or stolen mobile devices is an indication that businesses are instituting more safeguards to protect data on portable devices and limit the transport of that data off company premises by employees.

However, it appeared from a reading of these data breach incidents that none of the mobile devices involved in the breaches reported in 2013 were encrypted. By regulation, personal information must be encrypted if it is stored or carried on portable devices such as laptops, backup tapes, compact discs, flash drives or any other mobile device.

Employee Training

The regulations make clear that the onus of proper employee training in the handling of personal information rests with the employer. In fact, the regulations promulgated by the Office of Consumer Affairs and Business Regulation in March, 2010, mandate that any business that handles personal information must have a Written Information Security Program or “WISP.” Because employees’ information is also protected under the law, all businesses that employ Massachusetts residents need a WISP. Businesses, however, can customize their WISP based upon their size, resources, amount of data stored and the need for security and confidentiality of the personal information. A significant requirement of the WISP and responsibility of the business handling the personal information is employee training and monitoring of employee compliance. An observation that the Office has made in receiving data breach notifications since the inception of the data security law and regulation is that businesses are not consistent in implementing, promoting and maintaining regular employee trainings with respect to data protection.

Every business that owns, stores, maintains or possesses the personal information of a resident of the Commonwealth must acknowledge that it is entrusted with customer and employee information and has a responsibility to protect and maintain the integrity of that confidential information. Incidental to this is the recognition that the care with which a business trains its employees to guard personal information directly correlates to its reputation. Certainly, by implementing strict internal controls, and providing responsible oversight and proper training regimens for employees, companies could reduce or negate the occurrence of...the care with which a business trains its employees to guard personal information directly correlates to its reputation.
avoidable or negligent lapses and mistakes described in many of the data breach incidents that the Office received in 2013. As part of the business’s WISP, employees in every level of the organization should be educated, trained and encouraged to demonstrate and practice an awareness of the importance of the protection of personal information. Additionally, the business should be engaged in the reinforcement of privacy policies with its employees through practicing quality control measures, restricting access to sensitive personal information, conducting regular monitoring and providing explicit expectations of compliance.

In spite of a company’s efforts to practice all the measures listed above in order to protect the personal information to which it has been entrusted, the most basic, generic mistakes will continue to happen and data breaches will ensue simply because of the element of human error. For example, an employee may be enticed to click on a link that could lead to the exposure of vulnerable personal information, or an employee could act carelessly and become a conduit for an outside hacker to embed malicious software into the business network through phishing or a trick email.

Should a business suffer a data breach, its WISP and documentation of steps taken to guard and protect the personal information it retains or entrusts to a third party vendor and its response will be paramount in assessing its degree of culpability in the incident. It is not simply the careless mistakes listed above, but also more sophisticated and technical errors that may lead to a data breach. As reflected in the data breach incident reports throughout 2013, employees often unwittingly or unintentionally commit acts that compromise the integrity of personal information. Regular employee training and monitoring can greatly support an organization’s efforts in safeguarding personal information.

It appears evident from the information received by the Office in 2013 that most businesses continue to take positive steps towards safeguarding the personal information they own, store, license or possess. The number of data breaches involving mobile devices continues to decrease, and the number of Massachusetts residents affected by these incidents has decreased from 2012, until the 12th month of December when the Target breach took place.

The enormity of the Target breach serves as a reminder to businesses that they must create and maintain a WISP, continue to institute regular employee training, and conduct due diligence in their selection of data security-minded third-party vendors.

Businesses need to understand and appreciate that data breaches cut across a wide variety of sectors and that any organization is vulnerable, regardless of size. Planning and creating a culture of security may mitigate and perhaps contain the potentially disastrous effects of data breaches altogether.

**Conclusions**

To protect consumers’ personal information businesses will need to work closely with their employees to plan and create a culture of awareness and security.