2011 Data Breach Notifications Report

December 2011

2011 Report on Data Breach Notifications

History, Laws and Regulations

On October 31, 2007, the Commonwealth's Data Security Breach Law, Mass. Gen. Law c. 93H, went into effect. The law requires businesses and others who own or license personal information of Massachusetts residents to notify the Office of Consumer Affairs and Business Regulation and the Office of the Attorney General when they know of 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. Those who store or maintain such 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 a security breach? It is defined in the law as "the unauthorized acquisition or unauthorized use of unencrypted data, or of encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk or identity theft or fraud against a resident of the commonwealth."

What is personal information? The law provides a very specific definition: "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 Office of Consumer Affairs and Business Regulation's Data Security Regulations, 201 CMR 17.00, went into effect. The regulations require persons who own or license personal information about a resident of the Commonwealth to 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 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 important features of the Massachusetts law is a 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. While the definition of "encryption" is technologically neutral, it requires the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

The encryption requirement has been the law since March 1, 2010. Another important feature of the Massachusetts law is that the personal information of employees, as well as consumers be protected and included in the WISP.

The regulations also provide that persons owning or licensing personal information who hire 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 the 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.

In addition to the requirements to protect information

stored or maintained, a law regarding the proper disposal of personal information became effective on February 3, 2008, Mass. Gen. Law c. 93I. This law requires persons and agencies to properly dispose of records containing personal information. For paper documents, the law requires that records be redacted, burned, pulverized or shredded before disposal so that personal data cannot practicably be read or reconstructed. For electronic media and other non-paper media, the law requires that the media be destroyed or erased before disposal so that personal information cannot practicably be read or reconstructed. If an agency or person hires a third party to dispose of material containing personal information, that third party must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition or use of personal information during the collection, transportation and disposal of that personal information.

1,833

Total Number of Data Breaches Since November 1, 2007

3,166,031

Total Number of Massachusetts Residents Affected by Breaches Since November 1, 2007

Data Breach Notifications

Since the Data Security law, c. 93H, went into effect, the Office of Consumer Affairs and Business Regulation has tracked the data breach notifications it has received. As of Sept. 30, 2011, there had been 1,833 notifications of security breaches. The number of Massachusetts residents affected by the reported incidents since November 1, 2007 now totals 3,166,031. The reporting requirements of the law appear to reach all kinds of entities, as reports have come in from banks, government agencies, credit card companies, retail businesses, and the healthcare industry, among others.

2011

The reported breaches for 2011 continued, as in years past, to include a combination of criminal or malicious acts, poor data management practices, and errors in processing information.

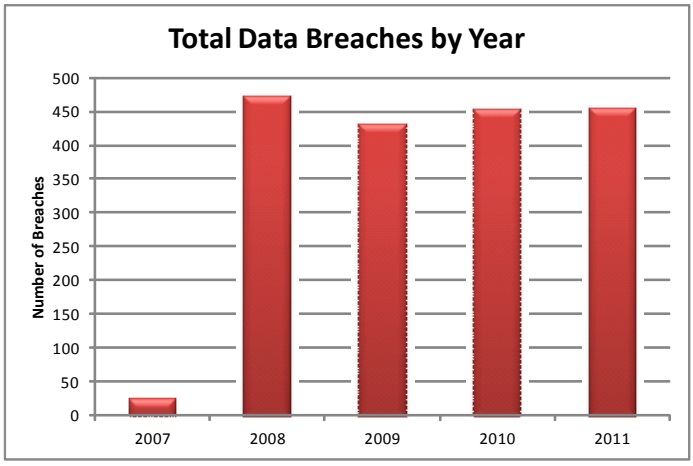
Criminal or malicious acts reported in 2011 resulting in breaches involved theft of personal information by a variety of means, including by outside intrusions into databases (often referred to as "hacking"), and the use of computer programs designed to access personal information without authorization (generally characterized as "malware"). The most widely publicized of the outside intrusions in 2011 involved the Sony PlayStation network incident, which affected 560,990 Massachusetts residents, of the estimated 70 million individuals affected worldwide. Another well-publicized breach in 2011 affecting persons both inside and outside the Commonwealth was the breach relating to certain shoppers at Michael's craft stores; 41,000 Massachusetts residents had their information compromised in these Michael's breaches. The Commonwealth itself also suffered a large malware data breach, affecting an estimated possible 245,000 residents, when a computer worm infected as many as 1,500 computers in the Departments of Unemployment Assistance and Career Services, from mid-April to mid-May of this year.

Also in the criminal or malicious category in 2011, there were breaches affecting smaller numbers of residents made by disgruntled former employees of businesses which held personal information who either retained access to data, or used the access codes of a former co-worker to gain access. OCABR regulations emphasize the importance of preventing terminated employees from accessing records containing personal information, and to the extent that one employee may know another's access codes, it is important to ensure

that such codes are also changed upon the departure of a terminated employee. Encrypting, and/or purging personal information that is no longer necessary to maintain, and immediately terminating access to information as employees leave the work force, could also act to limit such losses in the future. As of September 30, 2011, criminal or malicious breaches totaled 241 of 454 notifications received, 52.5 percent of total breaches reported.

Non-criminal or non-malicious breaches generally demonstrated poor employee or third party handling of residents' personal information, including transporting sensitive data in disregard of company policies, or in an environment without sufficient policies in place to secure the information. The three non-malicious breaches involving the largest number of Massachusetts residents as of September 30, 2011, affected almost 70,000 individuals. Those breaches involved unintended but preventable loss: the loss of "decommissioned" hard disk drives that were being transported from one out-of-state facility to another; a back-up tape that apparently fell into and was removed from the trash and disappeared; and the discarding of documents at a dump without shredding them or otherwise obliterating the personal information contained in them.

Some other non-malicious breaches involved the simple acts of placing the wrong document into the wrong envelope, or sending electronic attachments by e-mail to the wrong e-mail recipient, or losing a portable device. These two tables show that from November 2007 to September 30, 2011, almost 700,000



individuals were affected by non-malicious breaches. Non-malicious breaches are the most preventable breaches. This means either negligence or mistakes by employees or third party contractors resulted in exposing personal information for about 700,000 Massachusetts residents. This data reinforces the importance of employee training and the necessity of encrypting personal information transmitted over public networks or carried on portable devices.

Reinforcement of workplace policies concerning access to data, the importance of double-checking where information is being sent, and encrypting information sent wirelessly or by public network would have acted to prevent the instances which continue to crop up related to "wrong envelope," "wrong fax number" and "incorrect e-mail address" data breaches. While often only one person is affected by such errors, they are easily preventable by double-checking the addresses, fax numbers, and contents of the communication before information is sent out. Refresher courses on the written

Malicious Breaches

	2007	2008	2009	2010	2011	Nov. 2007-Sept. 2011 Total
Encrypted breaches	2	5	3	2	6	18
Not encrypted breaches	9	252	258	159	235	913
Residents protected by encryption	35	2,855	5,401	27	1,477	9,795
Residents compromised	**4,092**	**259,361**	**348,921**	**926,835**	**918,539**	**2,457,748**

Non-malicious Breaches

	2007	2008	2009	2010	2011	Nov. 2007-Sept. 2011 Total
Encrypted breaches	0	4	1	1	1	7
Not encrypted breaches	14	210	169	290	212	895
Residents protected by encryption	0	903	46	567	56	1,572
Residents compromised	**4,987**	**457,692**	**35,593**	**108,908**	**89,736**	**696,916**

policies of the employer that alert employees to the value of personal information to individuals whose information it is, the risk of criminal activity affecting those individuals if the information is lost, and their own obligation to safeguard that information, would likely result in fewer incidents still. Trainings that information sent wirelessly or through a public network must be encrypted should be a part of any WISP along with a special focus on lost or misplaced portable devices.

BREACH TYPE: ELECTRONIC, PAPER AND UNDEFINED

	Electronic Breaches	Residents Affected	Paper Breaches	Residents Affected	Undefined Breaches	Residents Affected
2007	20	8,635	7	114	2	2
2008	331	699,014	81	1,717	4	7
2009	324	347,828	106	5,737	6	220
2010	326	949,313	143	62,538	5	862
2011	364	1,075,157	106	14,878	8	9
TOTAL	**1,365**	**3,079,947**	**443**	**84,984**	**25**	**1,100**

Trends and Patterns

Generally, the data since November 1, 2007 demonstrates that many more individuals are affected at one time when the personal information at issue is kept in electronic files. Electronic files can be more easily protected than paper files by the simple step of encrypting them, and keeping encrypting tools up to date.

Both paper and electronic files can also be protected by limiting access to them, and destroying them once they are no longer needed. Electronic devices present unique challenges for transferring and disposing of personal information and consideration and forward-looking planning must be undertaken when putting together or revising one's written information security program. While misplacing a box of paper files may only impact a few hundred individuals, misplacing a DVD or hard drive could compromise the information related to thousands or even millions of individuals.

PORTABLE ELECTRONIC DEVICES

OCABR has also categorized breaches from portable electronic devices that were misplaced or lost and those that were stolen. We have also categorized the breaches by whether or not they were encrypted. If all portable devices were encrypted from 2007 to 2011, the number of residents whose personal information was compromised would be remarkably lower by 47 percent or 1,490,308 people. If all portable devices were encrypted from March 1, 2010 the number of compromised residents would have decreased by 29 percent or 909,992 people. It is clear that encryption of personal information on portable devices is still evolving and that more emphasis needs to be placed on accomplishing compliance with this feature of the law. It is also clear that compliance with the encryption requirement is a powerful tool to safeguard the personal information of millions of residents.

The breaches impacting large numbers of residents have been reported by a variety of sources, including health care providers, the financial services industry, educational institutions, retailers and government agencies.

Reporting Entities

Through September 30, 2011, the largest share of breaches were in the retail and healthcare industries, along with government. Most breaches reported by banks occur at payment processing centers and retailer establishments and are not caused by banks. Because banks own the compromised cards they must report the breach. A combination of computer intrusions by determined individuals and programs, and careless disposal practices were the causes of major losses of information. The contracting provisions required by March of 2012 should help insure that third parties and owners of information alike reaffirm their commitment to ensuring the "cradle to grave" protection of personal data.

Since the issuance of the Massachusetts regulations, the Office of Consumer Affairs and Business Regulation has conducted several seminars for businesses, developed and disseminated educational materials, and created the role of Data Security Ombudsman.

The Office of Consumer Affairs and Business Regulation's Deputy General Counsel has been

designated to provide assistance and work with the small business community to help with compliance. We have developed Frequently Asked Questions and a sample WISP to assist in this effort. These tools are available on our website. For further information please contact Deputy General Counsel Jason Egan at jason.egan@state.ma.us.

LOST OR MISPLACED DEVICES

	2007	2008	2009	2010	2011	Nov. 2007-Sept. 2011
Devices encrypted	0	0	1*	0	0	1
Devices Not encrypted	3	30	13	19	9	74
Total Lost or Misplaced Portable Devices	3	30	14	19	9	75
Residents protected by encrypted device	0	0	0*	0	0	0
Residents compromised	545	428,393	20,183	807,894	13,481	1,270,496

STOLEN DEVICES

	2007	2008	2009	2010	2011	Nov. 2007-Sept. 2011
Devices Encrypted	1	3	1	2	5	12
Devices Not encrypted	6	114	58	51	48	277
Total Stolen Portable Devices	7	117	59	53	54	290
Residents protected by encrypted device	33	2,840	37	27	1,173	4,110
Residents compromised	1625	81,887	47,683	74,150	14,467	219,812

*Company was unsure how many MA residents were affected in total.

Organization Breach Type for 2011

Organization Type	Total Reported	Total Residents
Commercial	19	44,840
Educational	24	8,459
Entertainment	10	652,169
Financial Services**	257	57,943
Food & Beverage	5	235
Health Care	63	72,561
Local Government	2	6
Manufacturing	4	983
Not-for-profit	4	65
Other	36	7,046
Pharmaceutical	1	70
Retail	2	2
State Government	18	245,104
Technology	12	844
Telecommunications	2	3
TOTAL	459	1,090,330

Organization Breach Type 2007-2011

Organization Type	Total Reported	Total Residents
Commercial	43	52,521
Educational	101	141,631
Entertainment	30	693,521
Federal Government	1	1
Financial Services**	955	901,156
Food & Beverage	35	11,453
Health Care	214	983,746
Local Government	7	1,850
Manufacturing	29	13,698
Not-for-profit	30	2,180
Other	164	44,289
Pharmaceutical	16	5,659
Retail	21	2,149
State Government	87	267,670
Technology	79	27,769
Telecommunications	17	7,018
Trade Union	4	9,720
TOTAL	1,833	3,166,031

**Breaches that are reported by banks are mostly debit and credit card breaches that occurred at payment processing centers and retail business establisments and are not caused by banks.