



Webinar Series

July 29, 2009

Preparing for the Strictest Privacy Law in the Nation:
MA Privacy Law 01 CRM 17

Presented by:



KNOWLEDGE MANAGEMENT ASSOCIATES, LLC

Agenda

- Overview of the new law and how it will affect your organization
- Discusses the anticipated implications from the new law and share some best practices around compliance
- 10 key questions to determine if you will be compliant by 1/1/2010
- A first look at a SharePoint-based compliance management solution to manage your program for CMR 17 compliance
- Next steps for you to take today



Law Overview

- Doug Cornelius, Chief Compliance Officer
- Publisher of *Compliance Building*

Compliance Building

Doug Cornelius on compliance and business ethics

[HOME](#) [SUBSCRIBE](#) [ABOUT](#) [DISCLAIMERS](#) [ARCHIVES](#) [TWITTER](#) [BLOG ROLL](#)



amazonkindle
Read my blog
on Kindle
Subscribe to have updates
sent to you

Latest Story

Ask for Usernames, Don't Ask for Passwords

Monday, July 20th, 2009 at 7:00 am

KMA

KNOWLEDGE MANAGEMENT ASSOCIATES, LLC

Disclaimer

- I am a lawyer, but I am not your lawyer.
- This overview is for information purposes. Please seek your own attorney for advice.
- These are my views and not necessarily the views of my employer.



Being a lawyer, I need to start off with a disclaimer.

I am not your lawyer, so seek your own legal advice and don't rely on slides from a free webinar.



Lets step in to way back machine to give you some background on why we are talking about a data protection law in Massachusetts.

TJX is the holding company for several retailers, so they have lots of financial account information.

Back in 2007 the TJX companies were subject to a data breach.

TJX
www.tjx.com

TJ-MAXX **Marshalls.**
T-K-MAXX **WINNERS**
HomeGoods **A.J. Wright.**
HOMESENSE **BOB'S STORES.**

Breach of data at TJX is called the biggest ever The Boston Globe
Stolen numbers put at 45.7 million

By Jenn Abelson, Globe Staff | March 29, 2007

At least 45.7 million credit and debit card numbers were stolen by hackers who accessed the computer systems at the [TJX Cos.](#), at its headquarters in Framingham and in the United Kingdom over a period of several years, making it the biggest breach of personal data ever reported, according to security specialists.

While details are still sketchy, TJX said unauthorized software placed on its computer systems stole at least 100 files containing data on millions of accounts from systems that process and store transaction information in Framingham and Watford, United Kingdom. Moreover, TJX believes the hackers last year had the capability to steal payment card data from its Framingham system as transactions were being approved. Even the files TJX tried to protect through encryption may have been compromised.

KMA
KNOWLEDGE MANAGEMENT ASSOCIATES, LLC

TJX took months to notify their customers that anything had happened.

The amount of information that was stolen was staggering. Over 45 million card numbers were compromised.

The current theory is that the bad guys sat in the parking lot of TJX and picked up the signal of an unsecure wireless router at TJX headquarters.

The screenshot shows a news article from The Boston Globe. The main headline is "TJX agrees to reimburse banks" with a sub-headline "\$40.9m will cover losses from fraud, reissuing of Visas". The article is dated December 1, 2007, and is by Ross Kerber. The text states that Framingham retailer TJX Cos. agreed to reimburse banks up to \$40.9 million as a result of the largest data breach in history, which compromised as many as 100 million credit and debit card accounts before it was discovered at the end of last year. A section titled "IDENTITY CRISIS" mentions that TJX, the parent of discount chains including TJ Maxx and Marshalls, reached a deal with credit card network Visa Inc. to pay some of the costs of reissuing cards and covering fraud losses at banks that issue Visa products, the two companies said yesterday. TJX also said it would help promote new security standards that Visa, MasterCard Inc., and banks have agreed to. To the right of the article, there are logos for TJ-MAXX, Marshalls, T.J. MAXX, WINNERS', HomeGoods, A.J. Wright, HOMESENSE, BOB'S STORES, and KMA (Knowledge Management Associates, LLC).

This was a disaster for TJX, having to pay millions to the banks affected.

The negative public relations with their customers was enormous.

TJX®
www.tjx.com

T.J. Maxx
T.K. Maxx
HomeGoods
HOMESENSE

Marshalls
WINNERS
A.J. Wright
BOB'S STORES

TJX faces class action lawsuit The Boston Globe
in data breach
Firm won't offer credit monitoring, CEO says in video

By Jenn Abelson, Globe Staff | January 30, 2007

A class action lawsuit was filed yesterday in US District Court in Boston accusing [T.J. Cos.](#) of negligence for failing to maintain adequate security of customer credit and debit card data and not disclosing the breach for a month.

The suit was filed on behalf of Paula G. Mace of Homer, W.Va., who had her debit card information stolen from the company's computer system. It is seeking credit monitoring services and any damages incurred by affected customers, according to Jonathan Shapiro, a partner with Stern Shapiro Weissberg & Garin of Boston, one of two firms that brought the case.

KMA
KNOWLEDGE MANAGEMENT ASSOCIATES, LLC

TJX was also subject to numerous civil suits for the loss of information.

TJX
www.tjx.com

T.J. Maxx **Marshalls**
T.K. Maxx **WINNERS'**
HomeGoods **A.J. Wright**
HOMESENSE **BOB'S STORES**

TJX to pay \$9.75m for data theft costs **AP** Associated Press
Associated Press / June 24, 2009
Email | Print | Reprints | Yahoo! Buzz | ShareThis | Text size - +

NEW YORK - The parent company of retailers T.J. Maxx and Marshall's will pay \$9.75 million in a settlement with several states related to a data theft that exposed tens of millions of payment card numbers.

Discuss **COMMENTS (1)**

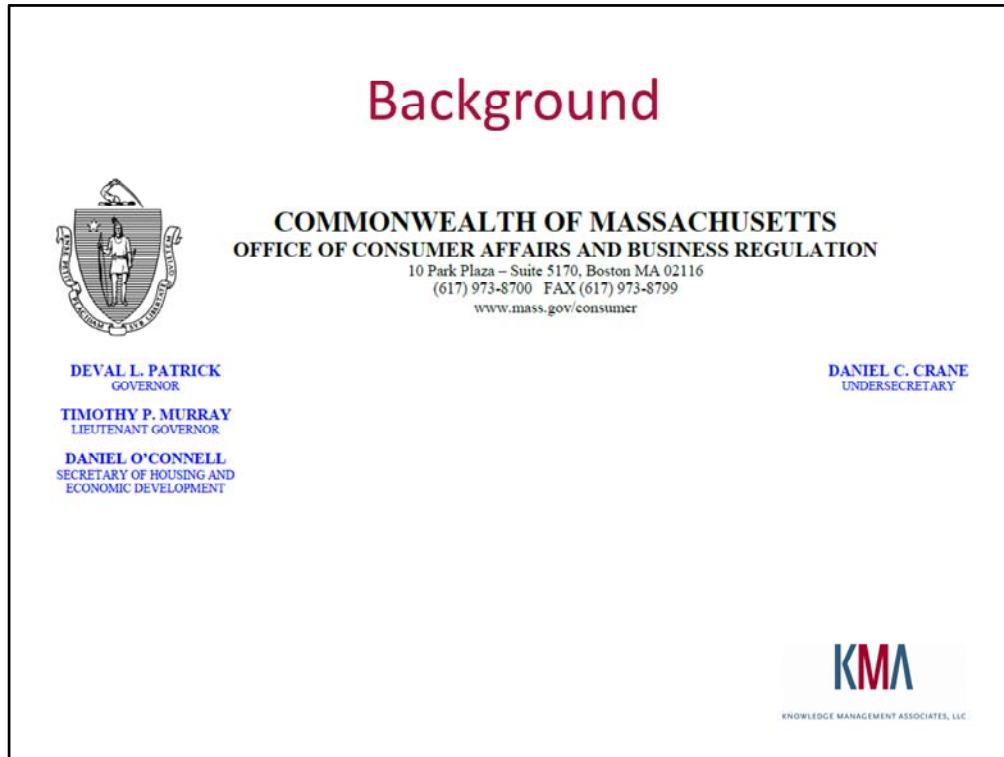
Framingham-based TJX Cos. said yesterday that it will pay \$2.5 million to create a data security fund for states, plus a settlement amount of \$5.5 million and \$1.75 million to cover expenses related to the states' investigations. But TJX stressed it "firmly believes" it did not violate any consumer-protection or data-security laws.

TJX said the settlement's costs are already accounted for in a 2007 reserve it created. According to documents filed with the Securities and Exchange Commission, as of May 2 - before the settlement was announced - the reserve was \$6.5 million, the company's estimate of the total potential costs related to

KMA
KNOWLEDGE MANAGEMENT ASSOCIATES, LLC

TJX also had to pay millions in fines to the state government.

The incident got the Massachusetts lawmakers focused on ways to protect the residents of the Commonwealth.




The state studied data breaches

During a 12 month period

There were

- 368 notifications of such breaches
- In only 11 of those was the data encrypted.
- In 77 of data breaches the data was password protected.
- 220 cases involved criminal/unauthorized acts, with a high frequency of laptops or hard-drives being stolen.
- Of the remainder, about 40% were the result of employee error or sloppy internal handling of information.

Background



COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
10 Park Plaza – Suite 5170, Boston MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer


DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

DANIEL O'CONNELL
SECRETARY OF HOUSING AND
ECONOMIC DEVELOPMENT

DANIEL C. CRANE
UNDERSECRETARY

**The breaches affected over
600,000 Massachusetts
residents.**

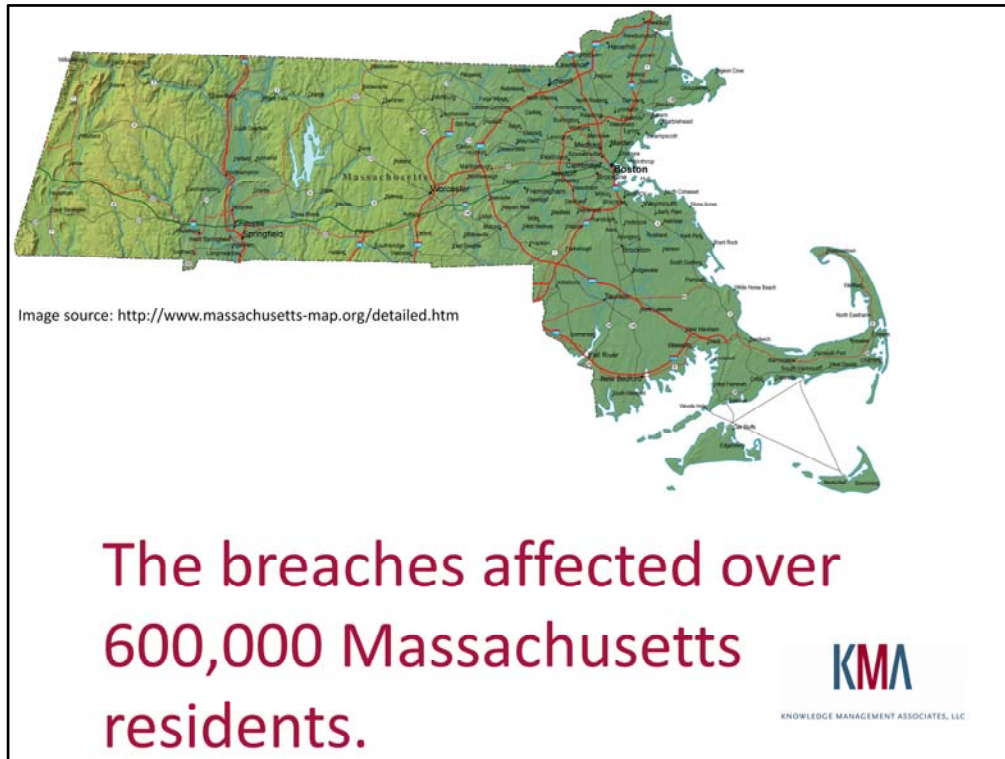


KNOWLEDGE MANAGEMENT ASSOCIATES, LLC

The breaches affected over 600,000 Massachusetts residents.

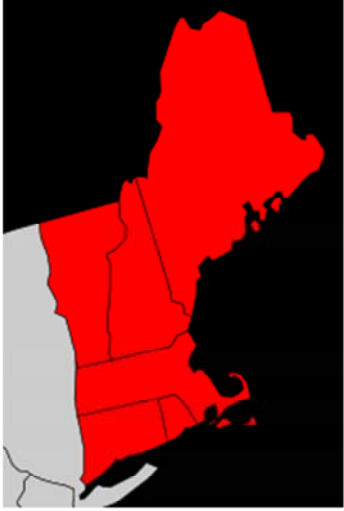
This confirmed to them that any regulatory regime must include measures that not only protect against intentional wrongdoing

BUT that also focus on internal protocols to set minimum security standards.




Just to emphasize, the Massachusetts data privacy law is focused on the residence of the person.

The law is in place to protect Massachusetts residents. The law is not restricted to businesses located in Massachusetts.




The breaches affected over
600,000 Massachusetts
residents.




That means it reaches beyond the borders of Massachusetts.

If you operate a business and you employ Massachusetts residents, you have personal information on your employees. You are subject to this law.



The breaches affected over 600,000 Massachusetts residents.



If you have personal information on your customers and any of your customers are Massachusetts residents, you are subject to this law.

That means that the Massachusetts law is the national standard.

Federal Regulation

- Gramm-Leach-Bliley
- HIPPA



What about the federal regulation?

What if you are a business that is already subject to Gramm-Leach-Bliley or HIPPA?

Those laws do not preempt state regulation in this area. The Massachusetts regulators are taking the position that their law merely clarifies the requirements of these federal laws.

Massachusetts Data Privacy Law

- Massachusetts General Laws
Chapter 93H
 - Statute on security breaches
 - shall provide notice, as soon as practicable and without unreasonable delay



The basis of the Massachusetts Data Privacy Law is Massachusetts General Law Chapter 93H.

This law focuses on notifications of a security breach.

Massachusetts Data Privacy Law

- 201 CMR 17.00
 - Regulations from 93H to safeguard the personal information of the residents of the Commonwealth



The statute also required regulations to safeguard the personal information of the residents of the Commonwealth.

Those came out a year ago as 210 CMR 17. They were revised earlier this year to reduce some of the limitations and to extend some of the deadlines for compliance.

Lets turn to some of the details of those regulations.

Personal Information

- Massachusetts resident's
- first name and last name, or first initial and last name
- in combination with:
 - 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)



We should start with the definition of personal information

There needs to be a Massachusetts resident involved.

There was some early chatter about segregating Massachusetts information from others. That turned out to be a bigger hassle than it was worth

You need that Massachusetts residents name associated with a social security number, State ID number, or a financial account number.

This breaks implementation of the law into two camps Human Resources and customer databases

Bob will focus on implementation later.

In dealing with the regulations, the implementation is going to be driven by the HR People responsible for employee records or by the IT people responsible for the customer databases.

Duty to Protect

- **Written Information Security Program**
- **Computer System Security Requirements**



The law has two overall requirements with the duty to protect personal information.

First, If your company owns, licenses, stores or maintains Personal Information about a resident of the Commonwealth you have to develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing personal information

And Second, if you electronically store or transmit Personal Information you also need to establish and maintain a security system covering your computers, including any wireless system,

Information Security Program

- Written



First off you need a written plan. Just in your head is not good enough.

Information Security Program

- Reasonably consistent with industry standards



You have to be reasonably consistent with industry standards, with enough administrative, technical, and physical safeguards to ensure the security and confidentiality of personal information.

Information Security Program

- Designee



You need to designate someone to be in charge of the program.

They don't need a particular title, like Privacy Officer.

But they do need to be clearly designated.

Information Security Program

- Identify and assess internal and external risks:
 - Employee training
 - Employee compliance
 - Detect security failures



You need to assess your risks and get employees involved in training, compliance and identification of failures and weaknesses.

Information Security Program

- Taking it outside



Develop a security policy about the transportation of records containing Personal Information outside of your business premises.

This is the lost laptop provision. There have been too many news stories about lost laptops containing Personal Information.

You need to address the question of whether that personal information needs to be stored locally on the laptop.

Information Security Program

- Discipline



The program needs to impose disciplinary measures for violations of the program rules.

The program needs teeth.

Information Security Program

- Terminating access for terminated employees



You need to prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to records. You need to immediately deactivate their passwords and user names.

Information Security Program

- Third Party compliance



In the original proposal, third party compliance was very controversial because the law required certification from third parties that handled your personal information records.

Now all you have to do is take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect that personal information in the manner provided for in the law.

It is a cascade requirement, that you can't get away from your obligations by handing the data over to a third party.

And of course, the third party is going to be subject to the Massachusetts law also.

Information Security Program

- Limiting the amount of personal information



You need to limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected.

You need to limit the time the information is retained to that reasonably necessary.

You need to limit access to people who are reasonably required to know such information.

Information Security Program

- Identify storage locations



You need to identify and determine which records contain personal information and where they are stored.

Information Security Program

- Restrict physical access



You need to impose reasonable restrictions upon physical access to records containing personal information

And you have to store the personal information records and data in locked facilities, storage areas or containers.

Information Security Program

- Monitor
- Review
- Document



Here is the compliance aspect.

You have to regularly monitor that the program is operating correctly and upgrade the safeguards as necessary to limit risks.

Review the scope of the security measures at least annually or whenever there is a material change in business practices that implicate the security or integrity of personal information records.

Document responsive actions taken in connection with any incident involving a breach of security.

Computer System Security



Let's turn to the security requirements if you store or transmit personal information electronically.

The regulations include the word "IF" but there are few companies with Personal Information that do not store or transmit at least some of it electronically.

Computer System Security

- Secure user authentication protocols



The law requires secure user authentication protocols

You need a secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices

You need to control passwords so that they are kept in a location and format that does not compromise the security of the underlying data

You need blocking access to user IDs after multiple unsuccessful attempts to gain access

Computer System Security

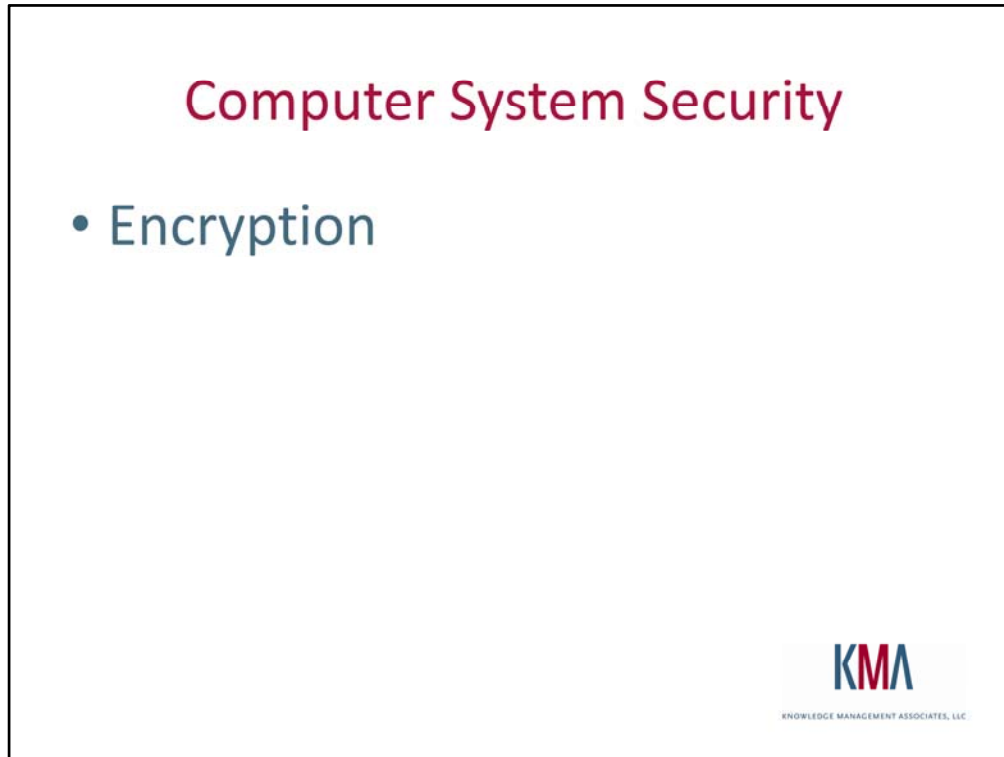
- Secure access control measures



You need to restrict access to records containing personal information to those who need such information to perform their job duties.

and

assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access.



To the extent technically feasible, you need to encrypt all transmitted records and files that:

contain personal information that will travel across public networks

AND

all data containing personal information that is transmitted wirelessly

AND

all personal information stored on laptops or other portable devices.

Computer System Security

- Monitor



You need to monitor your systems, for unauthorized use of or access to personal information;.

Computer System Security

- Virus Protection
- Firewall
- Malware



The law requires good protection measures

For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches.

You need reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions.

Computer System Security

- Training



Lastly, you need education and training of your employees on the proper use of the computer security system and the importance of personal information security.

Resources

- Massachusetts General Laws Chapter 93H
 - <http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm>
- 201 CMR 17.00
 - <http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf>
- Compliance Building Posts
 - <http://www.compliancebuilding.com/tag/mass-data-privacy-law/>



Implications & Best Practices

- PLACEHOLDER FOR BOB BOONSTRA



10 Key Questions

- PLACEHOLDER FOR SEAN MEGLEY



Compliance Mgmt Portal Sneak Peak

- PLACEHOLDER FOR SEAN MEGLEY

