

MASSACHUSETTS DATA PRIVACY: A PRACTICAL GUIDE FOR REAL ESTATE PROFESSIONALS

presented for
Northeast Association of Realtors
on
Thursday, May 20, 2010

presented by
John Rouleau
Computer Consulting Services
john.rouleau@verizon.net
Phone: (978) 337-8639

and

Scott C. Owens, Esq.
Attorney at Law
Email: scott@owensesq.com
Phone: (508) 733-6769

OVERVIEW OF MASSACHUSETTS SECURITY LAWS

- MGL c. 93H: Security Breaches
- MGL c. 93I: Disposition and Destruction of Records
- 201 CMR 17: Standards for the Protection of Personal Information of Residents of the Commonwealth

WHO MUST COMPLY?

ANY Business/Business Owner
INCLUDING Real Estate Firms and Independent Contractors

*Person: “A Natural Person, Corporation, Association, Partnership
or Other Legal Entity . . .” (MGL c. 93H, sec. 1)*

INCLUDING Out-of-State Businesses
IF Those Businesses Keep Massachusetts Resident Information

WHAT INFORMATION IS PROTECTED?

First Name/Last Name OR First Initial/Last Name

AND

Social Security Number

OR

Driver's License/State-Issued Identification Card Number

OR

Financial Account Number

SUCH AS . . .

- Customer Information
 - ▣ Deposit Checks (Name and Account Number)
 - ▣ Driver's Licenses (Name and License Number)
 - ▣ HUD Statements (Name and Account Number)
 - ▣ Payoff Authorizations (Name and Account Number and SSNs)
 - ▣ Documents for Short Sale Packages (Name and Account Numbers)
 - ▣ Etc.

AND ALSO . . .



- Employee Information
 - W2 Forms (Name and SSNs)
 - Direct Deposit Forms (Name and Account Information)
 - Drivers Licenses
 - Etc.

WHY IS THIS INFORMATION PROTECTED?

- ❖ TJX – over 100 million credit card numbers and hundreds of thousands of drivers license numbers compromised by hackers;
- ❖ Hannaford Bros. – 4.2 million credit card numbers compromised by hackers;
- ❖ Countrywide – former employee sold personal information of over 2.2 million customers;
- ❖ Bank of New York – personal information of 12 million customers compromised by lost back up tape;
- ❖ And, Don't Forget Departing Employees . . .

Departing Employees



- According to a February 2009 Study:
 - ▣ 59% of surveyed departing employees took sensitive and confidential data with them;
 - ▣ 89% of those who took data reported that their former employers did NOT scan laptops, portable storage devices or memory sticks for sensitive or confidential data;
 - ▣ Only 15% of surveyed companies audited paper and electronic records of departing employees;

WHAT MUST YOU DO TO PROTECT PERSONAL INFORMATION?

- **Maintain Control Over Electronic Information**
- **Maintain Control Over Paper Files**
- **Observe Proper Disposal Requirements**
- **WISP (Written Information Security Program)**

CONTROL OVER ELECTRONIC INFORMATION

- To be Established and Maintained “*To the Extent Technically Feasible*”, per 201 CMR 17.04:
 - Control Over Users/Control Over Passwords (17.04, 1)
 - Secure Access Control Measures (17.04, 2)
 - Encryption of Data (17.04, 3 and 5)
 - Travelling Wirelessly OR Stored on Portable Electronic Devices
 - Protection of Systems (17.04, 4 and 6 and 7)
 - Firewall
 - Security Patches
 - System Security Agent Software
 - Staff Education/Training (17.04, 8)
 - Proper Use of Computer Security
 - Importance of Personal Information Security

CONTROL OVER PAPER FILES

- Determine Reasonably Foreseeable Internal and External Risks to Files
- Store Paper Files in “Locked Facilities, Storage Areas or Containers”
- Restrict Access to Persons Who Must Access To Perform Job Functions
- Record Physical Safeguards in WISP

DISPOSAL OF PERSONAL INFORMATION

Check MGL c. 93I for guidance

- Separate Standards for Disposal of:
 - (a) Paper Documents
 - Redacted, burned, pulverized or shredded
 - (b) Electronic Media
 - Destroyed or erased
- In either case to such extent so that information is practically UNREADABLE or UNRECONSTRUCTABLE

USE OF THIRD PARTY SERVICERS



- Use of a 3rd party service is permitted provided the 3rd party has policies and procedures to prevent exposure of personal information during collection, transportation and disposal of material



WRITTEN INFORMATION SECURITY PROGRAM (WISP)

Pursuant to the Massachusetts Office of Consumer Affairs and Business Regulations (OCABR) standards, all covered entities must implement a comprehensive written information security program (WISP) by March 1, 2010.

What you need to do NOW!!!!



- Identify a Data Security Czar
- Audit Retention of Personal Information
- Identify Risks and Institute Appropriate Safeguards
- Implement Computer Security Procedures
- Ensure Employee Compliance
- Verify Compliance by Third Parties
- Establish Written Policies

What You Need To Do On An Ongoing Basis



- Continually Evaluate and Update Program
- Certify New Employees
- Debrief and Verify Compliance by Departing Employees
- Provide Appropriate Responses to Data Breaches

CONSIDERATION FOR CIRCUMSTANCES

Requirement of Reasonable Efforts to Comply

- Compliance Judged in Light of/WISP Contains Safeguards

Appropriate to:

- Size, Scope and Type of Service Provided
- Amount of Resources Available
- Amount of Stored Data
- Need for Security and Confidentiality of Both Consumer and Employee Information

NOTIFICATION OF BREACH (G.L. CH. 93H)

- When (to Send)
- (To) Whom
- What (to Include)
- What (Kind)

WHEN (to Send)

- Knowledge of Breach of Security
 - OR
- Knowledge that Personal Information Acquired/Used
- by Unauthorized Person/for Unauthorized Purpose

- “. . . as soon as practicable and without unreasonable delay . . .”
 - (MGL c. 93H, sec. 3)

(To) WHOM

- to Attorney General's Office;
- to Director of OCABR;
- to Consumer Reporting Agencies Identified by OCABR; and,
- to Resident(s).

WHAT (to Include)

- In Notice to Government (AG/OCABR):
 - Nature of Breach;
 - Number of Residents Affected; and,
 - Steps Taken/To Be Taken to Respond to Incident.

- In Notice to Resident:
 - Right to Obtain Police Report;
 - Process for Requesting Security Freeze; and,
 - Any Fees Required to be Paid to Consumer Reporting Agencies.
 - *BUT, DO NOT INCLUDE:*
 - Nature of Breach; or,
 - Number of Residents Affected.

WHAT (Kind)

Three Forms of Notice

- Written Notice;
- Electronic Notice
(consistent with Sec. 7001 of Title 15 of the USCS,
MGL c. 110G); or,
- Substitute Notice
IF cost of providing notice greater than \$250,000
OR affected class greater than 500,000
OR insufficient contact information.

PENALTIES FOR VIOLATION

Violation of MGL c. 93H

- Enforcement via MGL c. 93A
- \$5,000 Fine per Violation
- What is a “Violation”?
 - A Breach? A Breached Record? An Individual Resident Affected?

Violation of MGL c. 93I

- Not More Than \$100 per Resident Affected
- Not to Exceed \$50,000 for Each Instance of Improper Disposal
- What is an “Instance”?
 - A Record? A Device? A Series of Disposals?

WHERE DOES THIS LEAVE US?

□ Six Questions:

- What Information Do You Keep?
- Are You Careful About How You Keep/Send/Transport Data?
- Have You Created a WISP?
- Do You Limit Access to Your Data?
- Do You Oversee Your Employees and Third Party Providers?
- How Do You Dispose of Your Data?

□ Three Problems:

- Technology Regime Crafted by Lawyer-Legislators
- Lack of Specific Guidance
- Ad Hoc Decisionmaking

THE REAL QUESTION IS:

How Do You Comply, Technically
(Feasible) Speaking?

FINAL NOTE: FEDERAL RED FLAG



- Applies to “financial institutions” and “creditors”
 - ▣ No direct application to RE agents, but may impact lending-related aspects of your transactions
 - ▣ Awareness allows you to head off problems and/or advise/educate clients

4 Steps to Compliance



□ IDENTIFY

□ DETECT

□ PREVENT/MITIGATE

□ UPDATE

Identifying Red Flags



- Alerts, notifications and Warnings from Credit Reporting Agencies;
- Suspicious Documents;
- Suspicious Personal Identifying Information;
- Suspicious Account Activity;
- Notice from Other Sources;

Detecting Red Flags



- Multiple Document Verification
 - 2 forms of ID
- More extensive account authentication procedures
- Requirements for additional documentation

Preventing and Mitigating ID Theft



- ❑ Monitoring accounts
- ❑ Customer contact
- ❑ Password Changes
- ❑ Closing/freezing accounts
- ❑ Notifying law enforcement
- ❑ Placing accounts on “hold”

Updating Procedures



- Methods for stealing personal information are changing as quickly as procedures are put in place to protect the data;
- Continuously monitoring and updating procedures for effectiveness is necessary in this ever-changing environment;

QUESTIONS? CONCERNS?

Contact Us:

Scott C. Owens, Esq.
34 Hayden Rowe Street, Suite 168
Hopkinton, MA 01748
Email: scott@owensesq.com
Phone: (508) 733-6769

John Rouleau
Computer Consulting Services
Email: john.rouleau@verizon.net
Phone: (978) 337-8639