201 CMR 17.00 ID Theft Regulation

David Murray

General Counsel, Office of Consumer Affairs

Gerry Young

Secretariat Chief Information Officer (SCIO)

Executive Office of Housing & Economic Development

www.mass.gov

Agenda

- Legal Background to 201 CMR 17.00 (Massachusetts)
- Increasing Security Threat
- Security Process Begins with Encryption
- Holistic, Multi-Layered Security Approach
- Recommendations
- Questions & Answers

Legal Background to 201 CMR 17.00

- M.G.L. c. 93H – Legislature directed formulation of regulation.
- Goal is to protect the personal information of all Massachusetts residents.
- 201 CMR 17.00 established as a minimum standard.

Legal Background to 201 CMR 17.00

- Compliance is based on size, scope, and type of business; Resources available, amount and type of data stored.
- "*Personal Information*" is defined as *first name (or initial)*, and *last name*, PLUS ... *SSN, Driver's License number (or state-issued ID), Financial account number, or credit/debit card (with or without Pin)*.

Legal Background to 201 CMR 17.00

- Compliance Activities Required by Regulation:
- Written Information Security Program
- Identification of Records
- 3rd Party Providers must be evaluated for compliance
- Rethinking the Collection, Storage, and Access to PI
- Implementing and Monitoring Protective Measures
- Attorney General is tasked with enforcement of 201 CMR 17.00.

The Challenge – Rising Security Threat

- We hear every day about new security breaches.
- Blurring of Internal/External Networks and DMZs.
- Recent Verizon report shows a **three-fold increase** in breaches in 2008.
- Industry sources peg average cost per stolen record at ~ $202 (Ponemon Institute, 2009).
- There is news of hackers beginning to sell their offerings as Software as a Service (SaaS).
- Our adversaries are intent on breaching systems, and we need to become as serious, and determined as they are.
- 201 CMR 17.00 is currently the toughest ID Theft regulation in the United States (not the World, however).

The Security Process - Encryption

- Foundation of a sound security program is **encryption**.
- There isn't a breach that would not have been helped or mitigated by encryption use.
- In a world with *increasingly blurred boundaries*, encryption is prudent.
- Massachusetts has taken a deliberate vendor- and solution-agnostic approach. Form of encryption is up to the business.
- If there is no *personal information* … No encryption is required.
- Encryption encompasses both data at rest, and data in motion.

The Security Process - Encryption

- Magnetic Tapes that get rotated must be encrypted.
- You have a choice to classify your data, and encrypt only personal information, or declare all your data as containing PI and encrypt everything.
- We have advocated thinking about data inflection points … Safe at each point?
- We know encryption raises challenges, but we have to begin somewhere to draw the line in the sand. It will get honed & improved over time.

Holistic, Multi-Layered Security Approach[1]

- You are only as strong as your weakest link.
- Focus needs to cover Internal, as well as External threats (People, Process, and Technology).
- Look at your entire security model: Laptops, PDAs, Smartphones, Thumbdrives, Firewalls, IDS/IPS, DNS Servers, Routing & Switches, Authentication models, server hardening, etc. Whole disk encryption?
- Are you using Honeypots (traps) in your DMZ? Full-Duplex Taps? BlackHoles?
- Have you set up Trusted Domains so you can limit damage if you are breached?
- What condition is your Patch Management and Antivirus/Malware?
- What about Personal Information in your Database Tables?

[1] White, D., & Rea, A. (2008, Winter). A paradigm of network security design: A model for teaching network security. *Journal of Computer Information Systems*, 48(2), 54.