

Control Essentials

Volume II, Issue XI

November 2007

Business Consulting

- *Regulatory Support*
 - Policies and Procedures
 - Regulatory Compliance
 - Sarbanes-Oxley
 - GLBA
 - HIPAA
 - BSA
 - PCI (Payment Card Industry) Security Audit
 - Information System Audit Outsourcing
- *Enterprise Support*
 - Business Continuity Planning
 - Attestation and Assurance
 - SAS-70
 - E - Discovery
 - Forensic Examinations
 - Security Remediation

Technology Consulting

- *Application Security*
 - Application Security Assessment
 - Application Penetration Test
 - Web Application Security Assessment
 - Web Application Penetration Test
- *Network Security*
 - Risk Assessment
 - Vulnerability Assessment
 - Penetration Testing
 - Internal
 - External
 - Social Engineering
 - War Dialing
 - War Driving
 - Blue Snarfing
 - Wireless Security Assessment
 - Information System Security Audit
 - Information System Control Audit
 - Network Architecture Design and Assessment
 - Physical Security Assessment
 - Log Analysis

Florida Security Breach Notification Law

Background

Thirty-five states, plus the District of Columbia, have now enacted laws requiring businesses to provide notice of security breaches affecting personal information. California led this trend in 2003. Florida enacted its law in 2005. It is Florida Statute Section 817.5681.

The scope of the law

Private businesses: The law applies to any person who conducts business in Florida and maintains computerized data in a system that includes personal information. This law does not apply to governmental agencies, but it does apply to businesses that are providing government services under a contract with a governmental agency.

Unencrypted personal information: "Personal information" under this law means an individual's first name, first initial and last name, or any middle name and last name, in combination with any or more of the following data elements when the data elements are not encrypted:

- Social Security number.
- Driver's license number or Florida Identification Card Number.

Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Security breaches: "Breach" or "breach of the security system" under this law mean the unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person.



Security breaches trigger the law's requirements

Notices and disclosures must be provided when it is determined that there was a breach of the security of a system that maintains computerized data, and a Florida resident's unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notices and disclosures must be given within short time-frames

Law enforcement: The law does not directly set a time-frame for notifying law enforcement; however, the provisions of the law make it necessary to notify law enforcement immediately. The law requires that any notice and the timing of the notice be “consistent with the legitimate needs of law enforcement.” Also, the notification required may be delayed upon a request by law enforcement, if it is determined that the notification will impede a criminal investigation. The notification time period shall commence after the person receives a notice that the notification will not compromise the investigation.

The law also has special provisions for situations when law enforcement determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed.

Affected businesses: Any person that maintains data that includes personal information on behalf of another business entity must disclose any breach of security to the other business as soon as practicable, but no later than 10 days following the determination of the breach.

Affected Florida residents: Consistent with the needs of law enforcement, affected Florida residents must be notified without unreasonable delay, and no later than 45 days following the determination of the breach.

Consumer reporting agencies: If a breach requires notification of more than 1,000 persons at a single time, the person must also notify, without unreasonable delay, all consumer reporting agencies of the timing, distribution, and content of the notices.

The form of the notice to affected Florida residents

General requirements: The notice must be in writing. The notice may be electronic, if it is consistent with the provisions regarding electronic records and signatures in a federal statute referred to as the “E-Sign Act” and found in Section 7001 of Title 15 of the United States Code. The notice may also be electronic if the person or business providing the notice has a valid e-mail address and the affected person has agreed to accept communications electronically.



Alternatives allowed in some cases: Other types of notice such as publication with major state-wide media are permitted when the cost of providing notice would exceed \$250,000, the affected persons are more than 500,000, or the person does not have sufficient contact information.

Compliance with corporate security policy or applicable federal regulations: Businesses will be in compliance with the Florida law if they follow their own notification procedures that are part of its information security or privacy policy for personal information, as long as those procedures are consistent with the timing requirements of the Florida law. Also, businesses will be in compliance with the Florida law if they follow a notification procedure pursuant to the regulations or guidelines established by the business’ federal regulatory agency.

Penalties

Under this law, a person that fails to make the required notifications to affected residents or affected businesses may be liable for administrative fines. The fine is \$1,000 for each day the breach goes undisclosed for up to 30 days, and thereafter, \$50,000 for each 30-day period or portion thereof for up to 180 days. If notification is not made within 180 days, a person required to make notification is subject to a fine up to \$500,000 per security breach.

Note: Legislatures may revise or repeal a law. To see the text of the latest version of Florida laws, go to <http://www.leg.state.fl.us/statutes/>. The above summary is for informational purposes only. Enterprise Risk Management has helped organizations that have experienced a security breach with identification, containment, remediation and forensic expertise. Enterprise Risk Management does not provide legal advice. For legal matters, consult an attorney.

Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania
Syracuse University, Syracuse, New York
Xavier University, Cincinnati, Ohio
University of Miami, Miami, Florida
Florida International University, Miami, Florida

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.
Demotte Consulting, Ltd.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
CitiBank
Carnival Cruise Lines
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

enterprise risk management

The Control Professionals

800 S. Douglas Road, North Tower (# 835),
Coral Gables, FL 33134.
P: (305) 447 6750 F: (305) 447 6752
Email: info@emrisk.com Web: www.emrisk.com