

NAVIGATING TODAY'S DATA SECURITY ENVIRONMENT

MBA Legal Issues in Mortgage Technology

November 15-17, 2006

Marc Loewenthal

New Century Financial Corporation



A NEW SHADE OF BLUE CHIP™

- In 2005, 125 organizations reported security incidents involving 54 million individuals. Security incidents continue to be reported daily with the average cost of recovering from a breach continuing to rise - \$182 per data record or \$4.8 million per incident (Source: Ponemon Institute)
- 36 States have enacted breach notification laws – more states are expected to follow suit in 2007.
- 21 Federal bills have been introduced in the House and Senate.
 - » Some would preempt state law.
 - » Action now likely to occur in 2007 – 110th Congress.
- Most State laws are modeled on California's S.B. 1386 which was enacted in 2002 and are therefore similar but significant differences bear attention.

- **Requirements:**
 - » Notice must be given as follows:
 - **To California residents, without unreasonable delay, when their unencrypted personal information is believed to be acquired by an unauthorized person.**
 - **Notice may be in the following forms:**
 - › **Written notice, or;**
 - › **Electronic notice (but only if it complies with the federal Electronic Signatures Act which has specific requirements regarding verification of the identity of the consumer receiving the electronic notice and other requirements.)**
 - **Substitute Notice**
 - › **If written or electronic notice would be too costly (over \$250,000) or the number of individuals that must be noticed is over 500,000 or there is not have sufficient contact information, then substitute notice is allowed, as follows:**
 - › **E-mail notice, if the person or business has an e-mail address, or;**
 - › **Conspicuous posting of the notice on our Web site, or;**
 - › **Notification to major statewide media**
- **EXCEPTION:** If a Company has a notification procedure that is part of an information security policy that deals with the treatment of personal information and the Company complies with the timing requirements of the statute, then the Company may use its established notification procedures.

- Apply to breaches of unencrypted personal information
 - » Exception Example: Nevada includes all information, encrypted or unencrypted. (10/1/08)
- Speedy written notification following breach.
 - » Query – How fast?
- Personal information is defined as consumer name in combination with SSN, Driver's License or State ID, financial account or debit card number together with an access code.
- Delay in notification permitted if it would compromise law enforcement investigation
 - » Exception: Illinois
- Substitute notification via statewide media or website per CA standard
 - » Exception Examples: Rhode Island, Pennsylvania and Delaware
- Safe harbor if internal data security policies (which include breach notification) are consistent with state law.

State Law- Deviations From Common Themes



- 9 States have added a harm or risk threshold. If there is no reasonable likelihood of harm – no duty to notify.
 - » AK, Conn, FL, LA, MT, NJ, WA
 - » Query – how do you know?
- Safe harbor with regard to notification if the entity is covered by GLB, HIPAA, and/or Federal agency oversight and guidance – AZ, AK, Conn., LA, Minn., NV, NC, ND, TE.
- Coordination with Consumer Reporting Agencies regarding content, distribution and timing of notices to consumers.
 - » FL, GA, Minn., MT, OH, NV, NJ, NY, NV, TE, TX require some form of notification to the bureaus in some circumstances.
- Data destruction policies for data no longer required to be maintained - NJ.
- Ability to freeze credit bureau file – CA, NJ, VT,. 15 States have passed legislation.

- **Stricter requirements, harsher penalties.**
 - New York
 - › Covers unencrypted and encrypted data if encryption key has been compromised.
 - › Enforcement action permitted by State AG
 - › Content of notice is mandated
 - › Must also notify State Attorney General, Consumer Protection Board and cyber-security authorities.
 - › Must report large scale breaches to consumer reporting agencies.
 - › No exception for companies that have a plan to implement their own notification procedures pursuant to an information security policy.

- Preemption is needed – “floor” vs. “ceiling”?
- Triggers for notification. Is “substantial risk” standard the right one?
- Clear and concise definition of sensitive personal information.
 - » Increased protection for social security numbers.
 - » Ability for consumers to place credit bureau freezes.
 - » Giving consumers right to examine records held by data brokers and data collectors and correct inaccuracies.
- Who is covered?
 - » Data collectors and data brokers.
 - » Outsourced relationships - Who has ownership of a security breach?

- **Safe harbors.**
 - » GLB.
 - » Encryption.
- **Clear enforcement mechanisms.**
 - » State AG's.
 - » Coordination with local law enforcement.
- **Penalties**

- **Oversight agencies are OCC, OTS, FDIC, and FED.**
- **All have issued security guidelines that require financial institutions to have information security programs that:**
 - » Ensure the security and confidentiality of customer information;
 - » Protect against anticipated threats or hazards; and
 - » Protect against unauthorized access to confidential information which could result in harm to the customer.
- **Risk assessment and establishment of access controls is mandated by the guidelines.**
- **Components of incident response program should be:**
 - » Assessment of incident and type of information accessed;
 - » Notice to regulator of breach of sensitive customer information;
 - » Taking appropriate steps to control the incident;
 - » Customer notification where warranted; and
 - » Where appropriate, notification of law enforcement.

- **Notice to customers when sensitive information is breached.**
 - » Delay is warranted if notice would interfere with a criminal investigation – written request from law enforcement should be requested.
 - » Sensitive information is customer's name, address, or telephone number used in conjunction with customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to a customer's account.

- **Content of Customer Notice**
 - » Description of incident in general terms and type of information that was accessed;
 - » Action institution has taken to prevent further unauthorized access;
 - » Contact information for assistance;
 - » How to report any suspicious activity to the institution and credit reporting agencies;
 - » Reminder to periodically check credit reports, correct fraudulent information and place fraud alerts on credit bureau files;
 - » Provide information on identity theft and FTC's website and phone numbers in case assistance is needed.

- State laws will continue to proliferate modeled after California, New York and Interagency Guidelines.
- Federal legislation likely in 2007.
- Best practice for business entities doing business nationwide and not subject to a Federal regulator may be to pick the strictest of the state and proposed federal standards and incorporate them into a national program.
- What does this mean for your companies?

- **Comprehensive Information Security Policies and Processes are in Place.**
 - » Risk Assessments have been conducted.
 - » Capability to Correct Weaknesses During Normal Course of Business.
 - » Ability to Audit and Monitor.
- **Responsibilities are Well Defined and the Workflow is Established and Understood.**
- **Audit and Regulatory Concerns can be Resolved Quickly.**
- **Management Control and Accountability are Clear.**
- **See Financial Institutions Shared Assessments Program – FISAP at www.bitsinfo.org/FISAP/index.php for a good roadmap.**

- **Essential Elements:**
 - » Regularly Oversee Physical and Data Security Controls.
 - » Procedures for Transitioning Data are Understood and Implemented.
 - » Business Resumption Plans are in Place.
 - » Continuity Planning to Assure Continuous Protection of Data.
 - » Incident Response Plans and Contingency Arrangements are in Place and Tested in the Event of a Breach.
 - » Monitor Compliance with Applicable Laws and Regulations.
- **Evaluation of Third Party Providers.**
 - » SAS 70 Reviews.
 - » External Audits and Reviews.

- **Access to Third Party Provider Information.**
 - » If using a Third Party Provider that is Foreign, Data and Information Must be in English and Readily Available.
 - » Information Includes Contracts, Oversight and Audit Reports, Contingency Plans, etc.
 - » Design and Define Organizational Roles and Responsibilities.

- **Ability to Detect Intentional or Inadvertent Actions.**
 - » Inaccurate, Incomplete, or Unauthorized Transactions.
 - » Deficiencies in Safeguarding Assets.
 - » Deviations from Privacy and Information Security Laws, Regulations, or Policies.
 - » Don't Assume Perimeter Defenses are Enough.

- **Servers, Networks, Control Rooms and Databases**
 - » Limit Access to that which is Necessary to Support Responsibilities and Functions.
 - » Authorization System.
 - Controls Access to all Information.
 - Registers Each Individual.
 - Applications are Protected and Require Authentication to Access.
 - Staff Lists are Current.
- **Establish Information Classification or “Need to Know” Policies.**
 - » Information Should be Shared to Promote Informed Decision Making or Tasks Critical to the Services Being Provided.

- Information Security Protocols are Established with Respect to Design, Development, and Modifications for Enabling Technology.
- Change Control Procedures are Established and Followed.
- Systems Documentation is Complete.
- Incident Response and Reporting is Documented. Test your Response Plan.
- Intrusion Detection and Encryption are Employed where Feasible or Desirable.

- **Physical Controls**

- » Badge Access
- » Security Guards
- » Surveillance

- **Visitor Access**

- » Sign In
- » Badge ID
- » Escort when in the Facility

- **Environmental Controls**

- » Emergency Power-Off Switches
- » Surge Protectors
- » Fire Alarms
- » Smoke Detectors
- » Fire Extinguishers
- » Humidity Controls
- » Water Sources

- Background Checks – Check for Convictions for Fraud, Embezzlement, Larceny, Perjury, Terrorism, Breach of Trust or Fiduciary Duty.
- Training – Workflow, Security Standards, Information Classifications, Systems.
- Separation of Duties/Dual Custody of Information.
- Established Disciplinary Processes.
- Coordination of Functions Through Security Officers.

- Agree on Objectives.
- Establish Audit Processes.
- Work Out Notice Requirements/Timing.
- Provide for Reporting of Findings/Observations.
- Allowance for Response to Findings.
- Establish Cure Periods if Appropriate.
- Agree on Causes for Contract Termination if Critical Cures are not Undertaken.

- **Develop, Implement and Maintain a Plan.**
- **Establish Data Back-Up Protocols.**
 - » Software, Program Files and Data.
 - » Off Site Storage.
 - » “Hot Site” Should be Equally as Secure as Other Sites.
- **Set up Testing and Reporting.**
 - » All Parties Should Participate.
- **Resources to Execute Disaster Recovery Plan Should be Clearly Identified.**

- “Best Practices” are Employed.
- Customer Information Remains Confidential and Secure.
- There is Dedication to Planning and Detail.
- Customer Satisfaction Remains High.
- The Savings Potential is Realized from an Outsourcing Relationship if one is in place.