

# State Data Breach Notification Laws -- Update for Mortgage Lenders

Legal Issues in Mortgage Technology Conference  
Mortgage Bankers Association  
Phoenix, Arizona, November 15, 2006

**Jeffrey P. Marston, Powell Goldstein LLP**

**POWELL  
GOLDSTEIN** LLP

# What We'll Cover:



- **Reasons for explosion of security breach notification legislation**
- **Distinctions between the following types of state laws: (i) security breach notification legislation; these laws generally require companies and other entities that have lost data to notify affected consumers; and (ii) security freeze laws; these laws allow consumers to “freeze” or restrict access to their credit reports under certain conditions (only security breach notification laws are covered in this presentation)**
- **Relative dearth of federal law on this subject (but stay tuned!)**
- **Brief description of California SB-1386**
- **Common themes/issues in state legislation**
- **Additional issues to consider**
- **Some recommendations for managing compliance**

- **According to the Federal Trade Commission (FTC), the organization received 214,905 complaints of identity theft in 2003, up 40% from 2002.**
- **According to a federal bill currently under consideration, Congress estimates that nearly 10 million people were victims of identity theft in 2004 alone.**
- **In 2005, over 125 organizations reported security incidents involving over 54 million individuals.**
- **During 2006, the problem continues to grow, as evidenced by the ChoicePoint case and other breaches reported by the media.**

- **ChoicePoint Case**: On January 26, 2006, the FTC announced a record settlement in connection with consumer data broker ChoicePoint, Inc. regarding allegations that the company failed adequately to protect consumer data.
- ChoicePoint paid over \$15 million in civil penalties and redress and consented to a 20 year injunction requiring it to (among other things): (i) inspect its clients' facilities, (ii) conduct independent audits, and (iii) submit to extensive monitoring by, and reporting to, the FTC.

# Security Breach Headlines From 2006 (non-mortgage banking):



- Atlantis Resort in the Bahamas - **Reported January 8, 2006.** The personal information of **approximately 55,000 consumers** is compromised.
- San Jose Medical Group - **Reported January 19, 2006.** Former Office Manager indicted for theft of **medical records of 200,000 patients.**
- Notre Dame Donors Data Breach - **Reported January 24, 2006.** The personal information of **friends and alumni of Notre Dame University, who donated money to fund raisers, is compromised.**
- Ameriprise Financial Data Breach - **Reported January 26, 2006.** Laptop stolen and the personal information of **226,000 people** is compromised.
- Honeywell Data Breach - **Reported January 26, 2006.** Honeywell International, a **Morristown, PA-based industrial and aerospace conglomerate** that employs about 120,000 people worldwide, has personal information of **19,000 employees** compromised.
- Boston Globe Data Breach - **Reported on February 1, 2006.** Confidential information for **approximately 240,000 subscribers** is mistakenly distributed with Sunday newspaper bundles.
- Metro State Data Breach - **Reported on March 2, 2006.** Confidential information for **approximately 93,000 students** of Metro State College in Denver, could have been exposed.
- Georgetown University Data Breach - **Reported on March 6, 2006.** Confidential information such as **name, date of birth and Social Security numbers** of approximately 41,000 people has been exposed in the Georgetown University data breach.
- Department of Veterans Affairs – **Reported May 22, 2006.** Social Security numbers and other personal data belonging to millions of veterans were stolen from the home of a Veterans Affairs employee.

Many examples of data breaches involving banks, mortgage companies and financial institutions also exist!

---

## Risks And Costs Of Identity Theft

- In its 2003 report, the Identity Theft Resource Center estimates that victims of this crime spent an average of 600 hours, often over a period of years, reestablishing their credit and good name.
- As to the financial harm, Synovate, a research firm, in a FTC-sponsored survey, estimated that nearly \$48 billion in losses to businesses and financial institutions from identity theft occurred in a single year. It also found that consumer victims reported \$5 billion in out-of-pocket expenses for that period.

# Recent Study by Ponemon Institute

According to a very recent study by the Ponemon Institute (<http://www.ponemon.org/>):

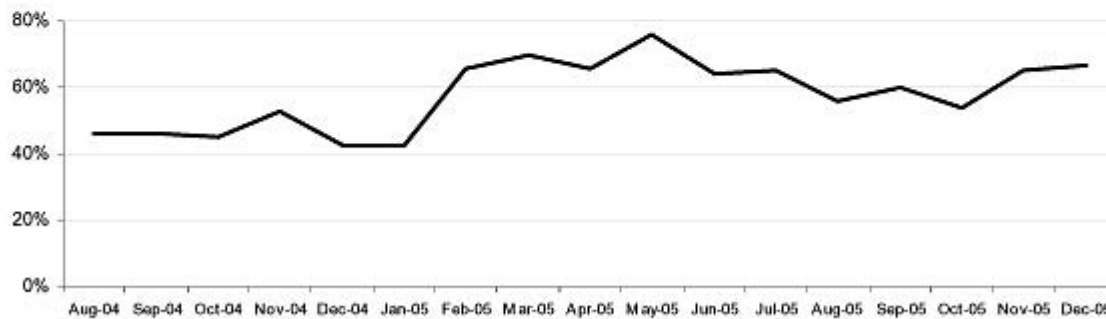
- Data breaches are very expensive, averaging \$4.7 million per incident; the cost is trending upward.
- Based on 31 real data losses, the study finds a surprising disparity between the financial impact of breaches and the amount spent on prevention. According to the study, the average cost is \$4.7 million per breach--an average loss of 26,000 records at a cost of \$182 per record—companies, however, spent only \$180,000 on preventing future data losses. Of the \$4.7 million cost, about \$2.5 million reflects the estimated cost of lost business.
- The cost of losing data rose significantly from 2005 to 2006. The 2006 average was \$182 per compromised record. The Ponemon Institute's 2005 study cited a lower figure of \$132 per record. These amounts include the cost of detection, escalation, notification, and follow-up help to victims.
- The study concludes that the "most salient costs result from the diminishment of confidence and trust in the company, which translates into abnormal or unexpected customer turnover. Our work supports the notion, 'an ounce of prevention is worth a pound of cure.'"
- Disclaimer: The study was sponsored by PGP Corporation and Vontu Corporation, security technology companies that stand to benefit from the findings if businesses decide to invest in an "ounce of prevention."

# Consumer Attitudes About Identity Theft



## Americans' fear about becoming a victim of identity theft

Percentage of individuals stating Yes or Unsure to the question:  
*Will you become a victim of an identity theft at some point in the future?*



- *“Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”* – renamed *“Interagency Guidelines Establishing Information Security Standards”* (see: 70 Federal Register 15736, 3/29/05, at <http://www.ots.treas.gov/docs/7/73262.pdf>; see also: <http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf>).
- *“Interagency Guidelines Establishing Standards for Safeguarding Customer Information”* (66 Federal Register 8616, 2/1/01) (<http://www.occ.treas.gov/fr/fedregister/66fr8616.htm>)
- **FTC’s Safeguards Rule:** The FTC requires non-bank “financial institutions” to develop a written information security plan describing their program to protect customer information. All programs must be appropriate to the financial institution’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue.
- **FTC Act (Section 5):** Unfair or deceptive acts or practices in or affecting commerce.
- The federal **Fair and Accurate Credit Transactions Act of 2003 (FACT Act)**, signed December 4, 2003, made significant changes and additions to the federal Fair Credit Reporting Act (FCRA). The Fact Act provides for free annual credit reports, increases the standard for the accuracy of information furnished to credit reporting agencies, strengthens adverse action notices, and creates a right to a credit score from a credit reporting agency for a reasonable fee. The FACT Act also adds (i) certain rights for identity theft victims and (ii) measures intended to prevent identity theft, including a duty on the part of creditors to take certain steps before granting credit when a fraud alert is contained in a credit file or accompanies a credit score. States retain significant authority under the FACT Act to continue to protect their residents, including from identity theft.

# Some Federal Preemption Likely; Timing Is Uncertain



- **Over 20 federal bills have been introduced in the House and the Senate. Some would preempt state law; others would allow states to provide additional consumer protections.**
- **No unifying federal data breach notification law (yet).**
- **In 2005, forty-seven state attorneys general sent a letter to U.S. Senate and House of Representatives leaders urging Congress to enact strong national security breach and credit freeze legislation to protect consumers from identity theft. The attorneys general expressed concern over the rapidly growing crime of identity theft, which they said costs their states over \$50 billion a year. They further warned Congress that if it cannot come up with a strong enough law, it had best leave the matter to the jurisdiction of the states. The letter opposed any move by Congress that would make the FTC the sole enforcer of any new security breach notification and security freeze laws, and spoke out against preemption of state laws. The AGs suggested that instead of full preemption, Congress should consider a “tailored” preemption of those states’ laws that are “inconsistent” with the federal laws, and then only to the extent of the inconsistency.**

# California Sets The Standard With SB-1386 (in 2002)



- California's Notice of Security Breach Act (commonly referenced as SB-1386/AB-700) was the first law of its kind and has been a bellwether for other states (and the federal government). Under SB-1386, any firm that owns or licenses electronic personal information must disclose any breach of the security of the system to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The ramifications of SB-1386 reach far beyond the state borders because the law applies to any organization that conducts business in California or with California residents.
- Encryption is the simplest, most effective way to achieve compliance with SB-1386. The law defines "personal information" as an individual's first name or initial in combination with other elements such as a Social Security number, driver's license number, account number or credit card number when "either the name or the data elements are not encrypted." (3 California Civil Code Section 1798.29(e).)

# California Sets The Standard With SB-1386 (continued)



- All encrypted data is thus exempt from the notification rules of SB-1386. The business and economic case for encryption becomes even clearer when one considers the expense of complying with these notification rules. Under SB-1386, affected organizations must provide one or more of the following when a security breach occurs:
  - » **1. Written notice**
  - » **2. E-mail notice**
  - » **3. Conspicuous posting of the notice on its public Web site or customer Web portal**
  - » **4. Notification to major statewide media**
- Gartner Research estimates organizations must spend at least \$90 per customer account to react to customer notification requirements. (Gartner Research, "Data Protection Is Less Costly Than Data Breach", 16 September 2005.) For example, a major financial institution allegedly spent an estimated \$7 million to comply with the notification rules after a single laptop computer (which contained unencrypted information for approximately 200,000 customers) was stolen.

# Other States Are Following CA's Example



- Over 30 states have now enacted some form of breach notification law; many more states have legislation pending.
  - » **Major problem:** state laws are local, but breaches are often national in scope. This presents a dilemma for companies with a national presence: do you adopt the most stringent elements of state laws until a federal standard emerges?
- Good sources for specific state law information:
  - » [http://www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf)
  - » <http://www.pirg.org/consumer/credit/statelaws.htm#breach>

- **“Triggering Events”**
  - » **A triggering event under state security breach statutes (*i.e.*, the event that gives rise to a consumer notice obligation) is generally the unauthorized acquisition of unencrypted computerized data, which acquisition compromises the security, confidentiality or integrity of an individual’s sensitive personal information.**
  - » **Such events potentially include almost any data breach, ranging from the accidental loss of a laptop computer to the intentional hacking of a computerized database.**
    - **Note that a triggering event might include unauthorized access by a company’s own employees (*e.g.*, in cases where the company’s privacy policy limits employee access and that policy is disclosed to customers).**

# Common Themes/Issues In State Legislation (Continued)



- Most state bills contain four main components. While a general discussion of these components follows, it is important to note that individual state laws have differing definitions and requirements.
- 1. Personal Information Definition – *What type of data is subject to breach law?* – An individual's name (or portion of a name) in combination with another identifying data element such as: social security number, identification card number, account or credit card number along with an access code or password, date of birth, biometric data, etc.
  - » Potential Issue – Although it may be relatively simple to associate an address with a person's name using a phone book, some states do not require notification if breached data includes paired social security numbers and addresses without a name.
  - » Potential Issue – Encryption language and definitions in some state bills lead to the question of whether compromised encrypted personal information constitutes a security breach.
  - » At least one state, Nevada, includes all information, encrypted or unencrypted. (Note, however, that a company that is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., is deemed to be in compliance with Nevada's notification laws; Nevada Senate Bill 347 (2005), Section 24(5)(b); see safe harbor discussion below.)
  - » Potential Issue – Does "personal information" include information that is fragmented throughout a document (*i.e.*, disassociated) if the breach also exposed the method to piece those data together? (In NJ, the answer is yes; in other states, such as PA, the answer is unclear.)

- **2. Notification Requirements – *Who is required to provide notification in the event of a breach?* – Any person or entity that conducts business in the respective state, and that owns, licenses, or is otherwise responsible for personal information data and reasonably believes that personal information has been acquired by an unauthorized person. Notice must generally be prompt (the “most expedient time possible and without unreasonable delay”) unless law enforcement notifies the institution that disclosure will compromise an investigation (practice tip: be sure to get this in writing from applicable law enforcement agency).**

# Common Themes/Issues In State Legislation (Continued)



- **3. Notification Procedures – *How are affected individuals to be notified?* – Data breaches meeting the applicable personal information definition and notification requirements must generally provide notice to affected individuals using one of three methods: (i) written notice, (ii) electronic notice with customer’s consent, or (iii) substitute notice (developed to handle large/costly breaches; usually allowed if the cost of providing notice would exceed \$250,000, the affected class would exceed 500,000, or the company doesn’t have sufficient contact information).
  - » **Potential Issue** – Several states do not require organizations to notify consumers of a breach if there is no “reasonable likelihood of harm” to the individual. The definition of “reasonable likelihood” is open to subjective interpretation by the organization that experienced the breach.**

# Common Themes/Issues In State Legislation (Continued)



- **4. Notification Timelines – *How quickly is notification required?* – This concept is vaguely treated in most legislation; consider, however, the laws in Florida and Ohio (45 days after the security breach). Many state laws use the California definition of “the most expedient time possible and without unreasonable delay” and include provisions for the needs of law enforcement.
  - » **Potential Issue – “Unreasonable delay” is a relatively subjective term. It may take months for an organization to assess the full impact of a large breach.****
- **Some states include more comprehensive provisions in their bills than those outlined above. Examples include requirements to secure and safeguard data, more rigorous definitions for personal information, data encryption and data disposal requirements, and consumer rights for credit freezes (*i.e.*, same statute covers breach notification obligations and security freeze obligations).**

- What constitutes a breach of security? Consider the factors of Materiality and Injury.
  - » Does the compromise of security have to be material in order to create a duty to give notice to consumers? Does the breach have to cause loss or injury (or do you have to reasonably believe that it will cause loss or injury) before a duty to give notice exists? At least 9 states have added a harm or risk threshold.

# Additional Issues To Consider (Continued)



- **Does the statute provide a private right of action for failure to give notice?**
  - » **In some states, only the Attorney General can bring an action for not complying with the notice statute.**
  - » **In other states, an intentional, knowing or reckless failure to give notice is considered a violation that imparts to consumers the right to bring action.**

## Additional Issues To Consider (Continued)

- **Are the statutes limited to imposing duties to give notice after a security breach?**
  - » **Some state statutes may also provide:**
    - **a mechanism for reporting identity theft incidents to the police,**
    - **a right to the state's residents to put a security freeze on their credit reports, keeping would-be identity thieves from opening new accounts, and**
    - **instructions on how Social Security Numbers can and cannot be used.**

# Additional Issues To Consider (Continued)



- Beware of so-called “second generation” statutes, which impose stricter requirements and harsher penalties. Example: New York statute (N.Y. Gen. Bus. Law §899-aa).
  - » New York law covers unencrypted and encrypted data if encryption key has been compromised.
  - » Enforcement action permitted by State Attorney General.
  - » 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.

# Additional Issues To Consider (Continued)

- **Potential Safe Harbors (at least in some states):**
  - **No notification necessary if entity is covered by (i) its own notification procedures (see PA example below), (ii) Gramm-Leach-Bliley Act, (iii) Health Insurance Portability and Accountability Act of 1996 (HIPAA) and/or (iv) federal agency oversight and guidance. Most important safe harbor is probably encryption.**
    - › ***E.g.*, Pennsylvania Breach of Personal Information Notification Act (BPINA) provides that (i) an entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of the BPINA will be deemed to be in compliance with the notification requirements of BPINA if the entity notifies subject persons in accordance with its policies in the event of a breach of security of the system; (ii) a financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with BPINA; and (iii) an entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional federal regulator will be in compliance with the BPINA.**

# Recommendation: Examine Laws And Prepare For Lawsuits



- **Develop a comprehensive security program for protecting all data, including personal information. Reference existing best practice standards, as many states identify best practice methods as a requirement. (For a discussion of one such best practice standard, ISO 17799, see: <http://www.computersecuritynow.com/presentation/index.htm>.)**
- **Develop data classification standards for identifying personal information, using broadest definitions of personal information.**
- **Conduct a risk assessment of all personal information.**
- **Include provisions for data security in contracts with third parties.**
- **Develop a policy for handling security breaches with a legal advisor. If appropriate, use attorney-client privilege when working with third parties, such as forensic investigators.**
- **Develop employee Q&A to respond to customer inquiries.**
- **Alert management, legal department and public relations department as soon as possible after a security breach.**

Atlanta ■ Washington ■ Dallas

One Atlantic Center  
Fourteenth Floor  
1201 West Peachtree Street, NW  
Atlanta, GA 30309  
Tel. 404.572.6600  
Fax. 404.572.6999



**Jeffrey P. Marston**  
**Powell Goldstein LLP**  
**jmarston@pogolaw.com**  
**202.624.3920**

901 New York Avenue, NW  
Third Floor  
Washington, DC 20001  
Tel. 202.347.0066  
Fax. 202.624.7222

JP Morgan Chase Tower - Suite 3200  
2200 Ross Avenue  
Dallas, TX 75201  
Phone: 214.721.8000  
Fax: 214.721.8100

[www.pogolaw.com](http://www.pogolaw.com)