



# The Law of Security Breach Notification

---

Reece Hirsch, CIPP, Partner  
Sonnenschein Nath & Rosenthal LLP  
Security Breach Notification 6 Years Later  
March 6, 2009

# California -- The Cutting Edge of Privacy Regulation

---

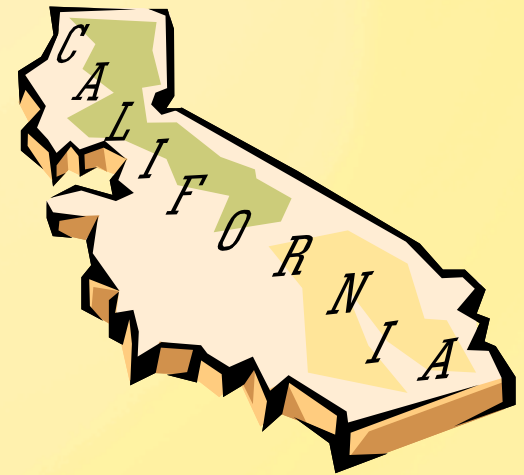
- California continues to be a trend-setter in privacy and security law.
- *A de facto* national standard.
- CA has often been a first-adopter of new types of laws that are later passed by other states, such as:
  - Social Security number disclosure
  - Security breach notification
  - Security freezes



# California – Hotbed of Identity Theft

---

- February 12, 2008: FTC report identifies ID theft as the number one complaint received by the agency in 2007.
  - The top 2 metro areas for reported ID theft complaints in 2007:
    - Napa, CA (302.6 complaints per 100,000 residents)
    - Madera, CA (280.2)
  - 16 of top 50 metro areas for ID theft complaints were in CA



# The Dreaded Security Breach



# The ChoicePoint Incident

---

- Four years later, ChoicePoint appears to be a watershed event in privacy regulation (and litigation).
- ChoicePoint, Inc. – one of the largest brokers of consumer data.
- By establishing at least 50 fake business accounts with ChoicePoint, criminals engaged in a massive identity theft scheme.
- ChoicePoint has identified at least 700 individuals who have been ID theft victims or attempted victims.

ChoicePoint



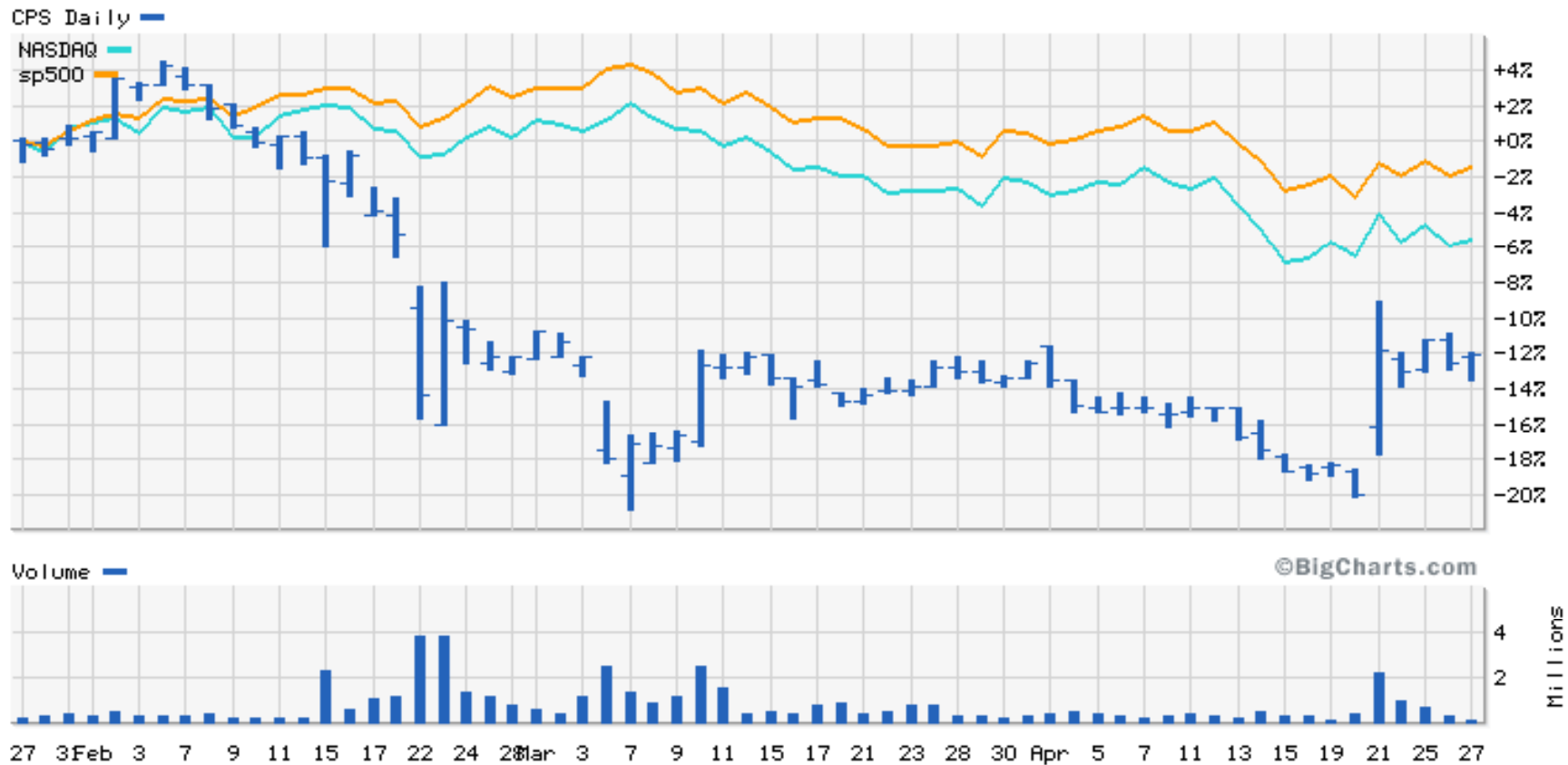
# The ChoicePoint Incident

---

- February 16, 2005 – ChoicePoint announces that it has sent notices to 35,000 Californians.
  - Ultimately learns that financial records of more than 163,000 consumers sold to possible identity thieves.
  - Notification process driven by California S.B. 1386.



# Security Breach Fallout - ChoicePoint



# The Aftermath

---

- Attorneys General from 38 states send letters to ChoicePoint demanding notification of affected consumers.
- February 2006 – ChoicePoint agrees to pay \$10 million fine, the largest civil penalty in the FTC’s history.
  - Also must create \$5 million fund for “consumer redress.”
- Current total – 45 states have enacted some form of breach notification law.
- Most are modeled after California’s SB 1386.

# The Lessons of ChoicePoint

---

- A sophisticated approach to privacy and security compliance is necessary because:
  - Identity thieves are becoming very sophisticated.
  - The potential damages (class action litigation, stock price, reputation, etc.) are enormous.

ChoicePoint



# Security Breach Notification Law

---

- Cal. Civil Code Section 1798.82.
- First-of-its-kind California security breach reporting law, requiring that:
  - any person or business conducting business in California
  - must report any breach of security
  - resulting in disclosure to an unauthorized person
  - of personal information in electronic form.

# Personal Information

---

- Section 1798.82 applies only to personal information of California residents.
- Does not apply if data is encrypted.
- Defined as:
  - First name or first initial; and
  - Last name;
  - Either Social Security number, driver's license number, or account number, credit or debit card number (with access code or password);
  - Medical information (since Jan. 1, 2008); and
  - Health insurance information (since Jan. 1, 2008).

# Notification

---

- Company must notify affected individuals if it “reasonably believes” that personal information has been acquired by an unauthorized person
- Company must disclose the breach to affected California residents “in the most expedient time possible and without unreasonable delay.”
- Content of notice is not specified, but may be in written or electronic form.

# Recommended Practices

---

- California Office of Privacy Protection issued recommended practices document.
- <http://www.privacy.ca.gov/recommendations/secbreach.pdf>
- Notification recommended within 10 days of breach.
- Theft or loss of laptops triggers notice.
- Recommended encryption: NIST's Advanced Encryption Standard.

# Contracting Issues

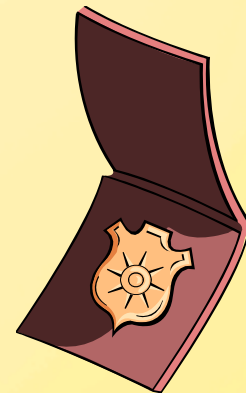
---

- Obligation to report security breaches under vendor agreement
  - Has vendor agreed to security incident reporting?
  - Coordinating notification process under Cal. Civ. Code Section 1798.82

# Notification Challenges

---

- Managing telephone inquiries from notice recipients.
- Providing information regarding credit bureau credit checks and fraud alerts.
- Should you provide a credit monitoring service?
- Coordinating with law enforcement.



# Class Action Lawsuits

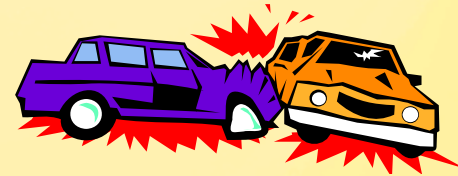
---

- Any customer injured by a violation of Section 1798.82 may bring a civil action to recover damages.
- An invitation to class action lawsuits?

# Most Common Mistakes In Security Breach Response

---

- Understand whether you are legally obligated to notify
  - Don't overreact
  - Can't “unring the bell” once a notification letter has been sent.
- Remember that state breach notification laws differ.



# Understand The Notification Triggers

---

- Is the company legally required to notify under applicable state breach notification laws?
- Understand the triggers.
  - Is “personal information” involved?
  - Has a “security breach” actually occurred?
  - Varying causation standards:
    - Is there a “reasonable belief” that information has been acquired by an unauthorized person (California)?
    - Is there a “likelihood of harm” (Delaware)?

# Beyond The Legal Analysis

---

- Legal obligation to notify is only the beginning of the analysis.
  - How would this incident be viewed by customers, public and press if it came to light?
  - The “front page article” test.

# Common Incident Response Mistakes

---

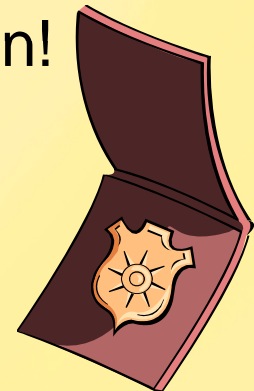
- In the heat of a crisis, organizations often forget that they adopted a security incident response plan.
- If regulators or plaintiffs in a class action charge that you acted unreasonably, being able to demonstrate that you followed a reasonable security incident response plan is a good way to show otherwise.



# Failing to Coordinate With Law Enforcement

---

- Consider whether it's appropriate to notify law enforcement.
  - Choose the right agency:
    - Local high tech crimes task force
    - FBI
    - Secret Service
    - National Infrastructure Protection Service
  - Don't use half-hearted law enforcement investigation as an excuse to delay notification!



# Other Common Incident Response Mistakes

---

- Failure to train your workforce to spot and report a security breach immediately.
- Failure to require prompt security breach notification in agreements with vendors/agents.
- Organize your incident response team in advance so that you're prepared to respond quickly.

# Other Breach Notification Measures

---

- Interagency Guidance on Consumer Data Breaches
  - March 2005 – Federal banking regulatory agencies issue interagency guidance on consumer data breaches
  - Proposed in August 2003, but quickly finalized in the wake of ChoicePoint.

# Other Breach Notification Measures

---

- The Health Information Technology for Economic and Clinical Health Act (HITECH Act)
  - Signed February 17, 2009 as part of stimulus legislation
  - Stringent and detailed breach notification provisions applicable to HIPAA covered entities and personal health record vendors
  - Interim final regulations due no later than August 17
  - Applicable to breaches discovered 30 days after issuance of regulations

# What's Next In Breach Notice Legislation?

---

- In the wake of TJX, several states are considering laws that would allow financial institutions to sue retailers and other merchants that retain customer payment card information that is breached.
- Minnesota was the first state to pass such a law in 2007.
- Efforts to pass general federal security breach notification stalled.



---

**For further information contact:**  
**Reece Hirsch, CIPP**  
**Sonnenschein Nath & Rosenthal LLP**  
**415.882.5040**  
**[rhirsch@sonnenschein.com](mailto:rhirsch@sonnenschein.com)**

Sonnenschein  
SONNENSCHHEIN NATH & ROSENTHAL LLP