Information Privacy Law.
Data Breaches and Identity Theft

Prof. Wendy Seltzer

18 U.S.C.§ 1028. Fraud and related activity in connection with identification documents, authentication features, and information

- Whoever …. (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; … shall be punished …

FTC Act, 15 U.S.C. § 45

- (a)(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

In re: BJ's Wholesale Club

- FTC Complaint (para. 7):
  - BJ's did not encrypt information in transit or in storage
  - Stored information in files that could be accessed with default user ID and password
  - Did not use readily available means to limit wireless access
  - Failed to employ sufficient measures to detect unauthorized access
  - Stored data up to 30 days when no longer needed

In re: BJ's Wholesale Club

IT IS ORDERED that Respondent, … shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the personal information collected from or about consumers…

"Identity Theft"

- A privacy problem?
- An authentication problem?
- A data security problem?

- Privacy Rights Clearinghouse chronology of data breaches
  - Running total number of records containing sensitive personal information involved in security breaches: 150,566,490

California SB 1386

- 1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

California SB 1386

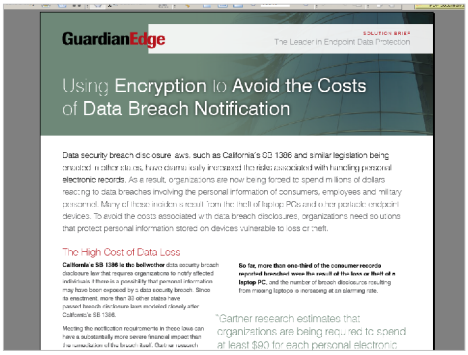
- To whom does it apply?
- For what activity?
- Who can enforce it?
- Whom does it help / hurt?

- What incentives does it create?
  - How can you avoid notification obligation?
  - How does the regulatory "hook" connect with its effect?

If you…

- Do business in California
- Collect personal information
- Permit access to unencrypted data
- by unauthorized person

You must notify California residents of unauthorized access to their PII


GuardianEdge

SOLUTION BRIEF

The Leader in Endpoint Data Protection

Using Encryption to Avoid the Costs of Data Breach Notification

Data security breach disclosure laws, such as California's SB 1386 and similar legislation being enacted in other states, have become vastly important initiatives associated with handling personal electronic records. As a result, organizations are now being forced to spend millions of dollars reacting to data breaches involving the personal information of consumers, employees and military personnel. Many of these incidents result from the theft of laptop PCs and other portable endpoint devices. To avoid the costs associated with data breach disclosures, organizations need solutions that protect personal information stored on devices vulnerable to loss or theft.

The High Cost of Data Loss

California's SB 1386 is the bellwether data security breach disclosure law that requires organizations to notify affected individuals if there is a possibility that personal information may have been exposed by a data security breach. Since its enactment, more than 30 other states have passed breach disclosure laws modeled closely after California's SB 1386.

Meeting the notification requirements in these laws can have a substantially more severe financial impact than the production of the breach itself. But we haven't

So far, more than one-third of the consumer records reported breached were the result of the loss or theft of a laptop PC, and the number of breach disclosures resulting from missing laptops is increasing at an alarming rate.

"Gartner research estimates that organizations are being required to spend at least $90 for each personal electronic

Effects

- Enable victims of data breach to take counter-measures
- Give access to data-breach information to
  - Journalists
  - Prosecutors / FTC
  - Private attorneys general (class action firms)
- Shame companies who fail to take precautions
- Establish standards of "reasonable" practices below which companies might be held negligent

Are data breaches good for us?