LORD BISSELL BROOK LLP

The Trend Towards Greater Liability for Security Breaches that Result in Loss of Personal Identifying Information

By:

Dave Leonard & John Kane

Security Breaches Leading to Potential Liability

- Hacking
- Employee theft
- Lost or stolen laptops, back-up tapes or CDs
- Poor Disposal of Sensitive Records

Security Breaches and Identity Theft

- A security breach can result in the loss or theft of personal identifying information, *i.e.*, Social Security Numbers
- Not every loss or theft of personal information results in identity theft fraud
- Increasingly, liability arises from security breaches which do not necessarily result in identity theft fraud

Liability for Security Breaches

- Three Sources of Liability:
  - Common Law (*i.e.*, tort-based negligence claims)
  - Contract
  - Statutes

The Courts' Initial Resistance to Claims Arising from Security Breaches

Common Claims Arising from Security Breaches

- Breach of fiduciary duty (special relationships)
- Breach of contract
- Negligence
- Invasion of privacy

Claimed Injuries Resulting from Security Breaches Not Resulting Identity Theft

- Cost of credit monitoring
- Loss of time
- Emotional distress damages
- Lost wages
- Out-of-pocket expenses
- Cost of credit checks and review
- Obtain new credit and debit cards
- Change direct deposit, withdrawal or transfer information

In the past, courts have denied claims because:

- Criminal acts generally are not foreseeable
- Courts found that there was no duty owed to keep personal data secure
  - No special relationship
  - No contractual duty
  - No statutorily imposed duties
- No recovery for threat of future damages
  - In absence of damages from ID Theft, courts would not award damages for mere threat of future harm

Recent Civil Cases

- Forbes v. Wells Fargo (Minnesota, USDC, 2005)
  - The plaintiffs sued Wells Fargo on behalf of a class of individuals whose personal identifying information was stolen when thieves stole 4 laptops from Wells Fargo
  - Court dismissed case because it found the plaintiffs injuries were all based on a "perceived risk of future harm," *i.e.*, that they may become victims of identity theft

Recent Civil Cases

- Guin v. Brazos (Minnesota, USDC, 2005)
  - Plaintiff sued company after laptops containing personal identifying information were stolen
  - Court dismissed case finding:
    - Theft was unforeseeable
    - Plaintiff could not demonstrate damages, because all she had was the fear that someone might use her information to commit fraud in the future
    - Company took “reasonable measures to maintain security of information”

Now, some courts are beginning to acknowledge that:

- Security breaches may be the foreseeable result of lax security practices
- Entities which require customers to provide personal identifying information have a duty to maintain that information securely
- A fiduciary relationship may arise when a company requires a customer to entrust it with personal information, and the customer reposes trust and confidence in company's superior expertise to maintain confidentiality of information

Recent Civil Cases

- Bell v. Michigan Council 25 (Michigan, App. Ct. 2005)
  - Court upheld $275K verdict against union for negligence in protecting personal information stolen by treasurer's daughter (court found 'special relationship' duty of care)
  - Found that it was **foreseeable** that personal information would be stolen as a result of allowing employee to regularly take laptop home which contained personal information of union members

Recent Civil Cases

- Jones v. Commerce Bancorp (New York, USDC, 2006)
  - Customer sued after her account information was stolen
    - Court recognized that plaintiff had a negligence claim and a breach of fiduciary duty claim
    - Court found that lost time and out-of-pocket expenses satisfied damages requirement
    - Court found that plaintiff was entitled to rely on bank's "superior expertise to safeguard her personal confidential information," giving rise to fiduciary relationship

Federal Statutes Which Impose a Duty to Maintain the Security of Personal Identifying Information

While not all of these federal laws provide for a private cause of action, courts may look to federal laws to determine whether a company owed or satisfied a duty of care to maintain the security of personal identifying information

Federal Statutes As Source of Duty

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Federal Trade Commission Act Section 5 (FTC § 5)

Gramm-Leach-Bliley Act (GLBA)

- Regulates financial institutions, requiring them:
  - to insure the security and confidentiality of customer records and information
  - to protect against any anticipated threats or hazards to the security or integrity of such records
  - to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

GLBA Safeguards Rule

- The GLBA contains a Safeguards Rule which requires financial institutions to develop a written information security plan that describes how the company protects its customers' nonpublic personal information. The Safeguards Rule also applies to information of individuals who are no longer customers of the financial institution

GLBA Safeguards Rule *(Continued)*

- The Safeguards Rule requires institutions to:
  - Designate at least one employee to manage the measures which safeguard nonpublic information
  - Construct a thorough risk management plan for each department handling nonpublic information
  - Develop, monitor, and test its measures which secure nonpublic information
  - Change the safeguards as needed regarding how nonpublic information is collected, stored, and used
    - The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes

HIPPA

- HIPAA requires that healthcare institutions take reasonable steps to limit the disclosure of an individual's personal health information, including training of employees to follow privacy procedures and securing access to electronic patient records

Sarbanes-Oxley Act

- Sarbanes-Oxley requires the CEOs and CFOs of publicly traded companies to ensure that their business processes have adequate internal controls
- This includes conducting an annual assessment of internal controls, including network security, relating to risk management

FTC §5

- Section 5 of the FTC Act prohibits unfair or deceptive trade practices
  - Using its authority under the FTC Act, the Commission has brought a number of cases to penalize as a "deceptive practice" a company's failure to abide by the promises in its privacy statements, including promises about the security of consumers' personal information
  - The Commission has also used its authority to penalize as "unfair practices" information security practices that cause substantial consumer injury

Examples of FTC Act § 5 Actions

- FTC Action Against BJ's Wholesale Club (Washington, D.C., January of 2005)
  - Complaint is the first based on "unfair" rather than "deceptive" trade practices
  - FTC charged that BJ's engaged in unfair trade practices by failing "to employ reasonable and appropriate measures to secure personal information"
    - $13M in fraudulent credit & debit card charges caused by the transmittal and storage of data from credit card magnetic stripes over unsecured wireless network
    - FTC settlement requires encryption, data retention rules, better password procedures, incident response, biennial security audits and reports for 20 years

Examples of FTC Act § 5 Actions

- FTC Action Against ChoicePoint (Atlanta, Georgia, January of 2006)
  - Complaint contains claim for “deceptive” trade practices
  - FTC charged that ChoicePoint engaged in deceptive trade practices by failing to employ reasonable and appropriate measures to secure personal information, in violation of statements contained in ChoicePoint’s privacy statements
    - Paid $10 million in civil penalties and $5 million in consumer redress to settle FTC charges and agreed to various measures to ensure security of confidential information

STATE LAWS REGARDING THE MAINTENANCE AND DISPOSAL OF PERSONAL IDENTIFYING INFORMATION

While the features of each state's laws vary, increasingly, states are acting to provide civil remedies and penalties for security breaches which result in the loss or theft of personal identifying information

Features of State Laws

- Security Breach Notification
  - Security Breach Laws require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised lost, or stolen. So far, 34 states have passed a notification law

Example of Security Breach Notification Law

- California's Security Breach Information Act:
  - Mandates public disclosure of computer security breaches in which confidential information of any California resident may have been compromised
  - Covers every enterprise – public or private, regardless of location – doing business with California residents
  - Violators could be liable for civil damages or face class action lawsuits

Other Features of State Laws

- Credit monitoring requirements
- Safeguards for destruction of personal records
  - Requires government and businesses disposing of personal information to take reasonable steps to protect against unauthorized access
- Protection of Social Security Numbers
  - Restricts government and business use of social security numbers on records made available to general public

Other Features of State Laws

- Security freeze
  - Consumers can freeze access to their consumer credit report and credit score. Without this information, a business will not issue new credit in a consumer's name. When a consumer wants to get new credit, he or she uses a PIN to unlock access to the credit file
- Civil penalties
- Create private causes of action
- Authorize recovery of attorneys' fees
- Authorize class actions

Going Forward, We Can Expect

- More state laws that establish a duty providing a basis for plaintiffs to sue
- More state laws that provide for civil penalties and create private causes of action
- More pressure for the enactment of a federal law with uniform standards and penalties
- More cases in which courts recognize a common law duty to maintain the security of personal identifying information

LORD BISSELL BROOK LLP

Questions?

Dave Leonard, Esq.
Partner
Phone: 404-870-4676
dleonard@lordbissell.com

John Kane, Esq.
Associate
Phone: 404-870-4663
jkane@lordbissell.com