BECKER & POLIAKOFF
Legal and Business Strategists

Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend A Claim

By Wayne M. Alder
walder@bplegal.com
561.655.5444

"There are only two types of companies: those that have been hacked and those that will be."

-Federal Bureau of Investigation Director Robert Mueller. [1]

In today's world, no one is immune from the risk of a data breach. Hardly a week will go by when the news does not report on a company or government entity suffering a catastrophic loss of private and privileged confidential personal data. These losses are not just happening to the unsophisticated, but to major companies and organizations. In June of this year the Federal Government's Office of Personnel Management suffered a data breach that exposed the personal data of at least 4 million current and former federal employees.[2] The loss of information from Sony Pictures, Target, and many others highlights that no organization is immune.[3] A study by the Ponemon Institute out of Michigan found that the average cost of a corporate data breach last year was $3.5 million.[4] The U.S. Department of Defense noted that "[e]very year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies."[5] For anyone doing business today, an understanding of the basis for potential liability—both statutory and civil—for such losses of information is essential, not only to limit liability or to keep your organization out of the news, but to protect and professionally service your clients and business partners.

COMMON CAUSES OF DATA BREACH

Numerous studies and extensive research by insures and computer securities experts have pinpointed the eight most common causes for a data breach. While not exhaustive, these "eight sins" of computer security provide an excellent understanding of the mechanics of a data breach failure:[6]

1. **Weak/Stolen Credentials (Passwords)**
   Weak or lost passwords are the key that unlocks to door to a computer system for maleficent outsiders. Studies show 4 out of 5 breaches systems are caused by this, which makes sense, as even the most sophisticated system remains vulnerable if the bad guys are given the keys.

   Solution: Use Complex passwords. Never share passwords. Update and change Passwords on a regular basis. Constantly remind users to protect passwords and system protocols.

2. **Back Door Failures**

   These failures occur when a weakness in a program or protocol exist, opening the door to outside world. Such failures are constantly being probed and tested by hackers for vulnerabilities, and they often allow them to bypass passwords and security protocols.

   Solution: Maintain updates and patches on all software and hardware.

3. **Malware**

   Although not strictly a "virus", malware is, by definition, malicious software that is loaded without knowledge of its true impact or intent. It is often hidden in a program a user thought was beneficial. Hidden behind such "useful" programs, the malware opens up access points to exploit a system.

   Solution: Strictly prohibit employee downloads of non system programs. Do not open emails where their origin is unknown. Never install programs sent by email or email link. Maintain a rigorous anti-malware scanning system regiment that is updated often.

4. **Social Media/Scams/Phishing**

   Either through social media or emails, hackers will try to gain access to closed systems through elaborate ruses or promised monetary gain. Through such means an employee will be convinced to provide an access point to the outsiders or to provide security keys or passwords.

   Solution: Constantly remind users to never share passwords or protocols to outsiders.

5. **Numerous Permissions**

   Large numbers of full permissions in use are a boon to hackers, as each one represents the keys to the kingdom. With a great number of full access permissions in use, a business is more likely to lose track of who has the permissions, and fail to close accounts of ex-employees.

   Solution: Where possible, provide limited permissions to users. Where full permissions are required, strict control and monitoring is required.

6. **Insider Threats**

   This comes in two varieties: The "careless" and the "rogue". The careless employee will provide his password or system protocols to outsiders, not for a malevolent purpose, but out of ignorance of the repercussions. The rogue will seek to exploit his or her knowledge of the system with the intent of causing harm.

   Solution: Maintain employees' awareness levels on the importance of system security, including password protection to ward against the careless employee. To deal with the rogue employee, monitor system use. When uncharacteristic use is detected, investigate. Do not delay to deny system access when any indication of a problem arises. Shut down access to terminated employees promptly.

7. **Physical Vulnerability**

   An open desktop is a portal to your system. A system left on after hours in an unsecured location makes it easy for someone to gain access and download data.

   Solution: Maintain and control the physical building and access. Secure or log off systems that are not in a secure location.

8. **Improper Configuration**

   A system is only as good as its protocols, hardware and programs. Outdated or subpar designs of hardware and programs are chum in the water to the hungry cyber shark.

   Solution: Professional design and management of hardware systems is a must. This is not an area where the "jack of all trades" businessman or woman should tread. The money spent on professionals will provide dividends for you, your business, customers and business associates and provide confidence in you and your organization.

As Ken Schultz, the Chief Information Officer/Chief Technology Officer of Becker & Poliakoff, P.A., noted, "We are in a world where we often have the need to access data anytime, anywhere and from any device. Providing that type of convenience, while protecting important data, is a full time job that requires a great deal of experience from systems professionals. We so often see companies with poorly conceived systems, plans and policies that virtually invite problems to happen." At Becker & Poliakoff, P.A. the firm implemented a Computer Security Training course mandatory for all employees, which reinforce the lesson that most breaches are due to careless human error, and serves as additional training to protect the firm and its client's information.

STATUTORY AND CIVIL LIABILITY

The recent increase in the number of cyber-attacks has been matched with an increase in liability to companies and individuals for related data loss. Two types of legal liabilities generally arise from data breaches: statutory and civil. While both will impose liability on the unprepared, the manner of liability and how corporate counsel can protect their companies differ widely.

STATUTORY LIABILITY

Statutory liability for a data breach comes in two forms: federal law and state law. The federal Gramm-Leach-Bliley Act requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.[7] The Health Insurance Portability and Accountability Act of 1996 ("HIPPA") contains specific privacy and security rules which mandate 'encryption and protection of patients' electronic protected health information (ePHI) held on networks. Repercussions for HIPAA violations related to data breaches can be severe. Recently two health care organizations agreed to settle charges that they potentially violated theses safeguards and agreed to monetary settlements of a combined $4,800,000—the largest HIPAA settlement to date.[8] Additionally, the regulatory duties and liability companies are now exposed to come in many additional forms, depending on the specific nature of the business. A data breach may require disclosure to various federal agencies including, but not limited to: the Securities Exchange Commission (SEC)[9], Federal Trade Commission (FTC)[10] or the U.S. Department of Justice.[11]

In addition to the federal mandates, 46 states, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.[12]

Florida's law is a good example of the type of state law imposing liability and penalties for a data breach as it is one of the strictest in the nation. In Florida, where the home office of Becker & Poliakoff, P.A. is located, a new statute defining what is "protected data" and imposing penalties for failure to take action after a data breach came into effect in July of 2014. The law, signed by Governor Rick Scott on June 20, 2014, is called the Florida Information Protection Act of 2014 or "FIPA." The law is one of the strictest enacted in the United States. FIPA repealed Florida's prior data breach notification statue, FL. Stat. § 817.5681, and replaced it with § 501.171, and made modifications to Florida law to reach businesses, government and other entities outside the state.

FIPA provides, like the prior statute, that "personal information" includes first name or first initial with the last name; social security number; driver's license number or other government-issued ID number: financial account number; or credit or debit card number with security codes. FIPA added that "personal information" will now also include any information about an individual's medical history, mental or physical condition, or medical treatment/ diagnosis; or health insurance policy number or subscriber identification number, and any "unique identifier" used by a health insurer. FIPA further enlarges the definition of "personal information" to include any information that would allow access to an online account. Of importance is that this enlarged definition would include log-in information for social media platforms such as Facebook or Twitter. This appears to be the broadest definition of "personal information" in the United States. The exception to "personal information" covered by FIPA is information already made public or information that is encrypted.

FIPA covers all commercial or governmental entities that acquire, maintain, store or use personal information of individuals in the state. Importantly, FIPA did away with the language limiting Florida's protection of a breach of personal information to those who "conduct business" in the state alone. Thus, companies in other jurisdictions, including internationally, should assume this statute will apply if a breach of security occurs which affects any Florida resident.

Under FIPA, the time period to report a breach of personal information has been reduced from prior Florida law to 30 days from the time the breach is discovered. However, the statute authorizes the Department of Legal Affairs to grant up to 15 additional days to provide notice for good cause if the request for extension of time is provided in writing to the department within 30 days of the breach.

If 500 or more persons are affected by the breach, FIPA requires that notice also be provided to the Florida Department of Legal Affairs. If the breach affects 1,000 or more persons, additional notice must be given to all nationwide consumer credit reporting agencies.

No such notice is required to affected individuals if, upon conducting an investigation and consultation with law enforcement, it is reasonably determined that no affected individual "has or is likely to suffer identity theft or any other financial harm." However even "where no harm" has been determined, the covered entity must still provide a written notice to the Florida Legal Affairs Department within 30 days of the determination that "no harm" occurred. In all

cases of a data breach any law enforcement agency may order a delay in providing notice if the law enforcement agency makes a determination that such notification would interfere with a criminal investigation. Thus FIPA mandates prompt coordination with law enforcement after a breach.

Third-parties that maintain "personal information" for a covered entity that suffer a data breach have 10 days under FIPA to report the breach to affected covered entities. Following receipt of this notice, a covered entity becomes responsible under FIPA for providing any necessary notice within the 30-day notice period as required by the statute. Although FIPA specifically mandates that it does not create a private cause of action, the statute authorizes the Florida Department of Legal Affairs to bring an enforcement action against covered entities. Failure to provide adequate notice under FIPA is a violation of the Florida Deceptive and Unfair Trade Practices Act and is subject to following civil penalties:

- $1,000 per day for the first 30 days
- $50,000 thereafter for each 30-day period or portion thereof for up to 180 days
- $500,000 as the maximum amount of total penalties for violations continuing more than 180 days

Accordingly, faced not only with federal law, which will vary depending on the type of information your business is dealing with, but state law that will vary widely depending on the locality of your business, the first step for any corporate counsel for a business entity operating with information of customers, consumers, clients, patients or the public of any kind should be to seek advice from outside counsel within their state as to the requirements and liability required by the federal government for the type of business it is engaged in, and the statutory requirements mandated by the state it operates in.

However, state and federal statues are not the only foundation of liability for a computer breach. Aside from liability imposed by statute or code, civil actions based upon contract and tort claims are common against companies that have suffered data breaches.

CIVIL LIABILITY

Typically plaintiffs bring contract-based actions when data breach occurs based upon a contractual promise to protect personal information. Where no specific terms in the contract regarding protection of personal information exist, savvy plaintiffs will point to promises made to protect personal information and attempt to incorporate such promises into the terms of the contract. Moreover, plaintiffs are increasingly claiming that an "implied contract" exists to safeguard data if such data is collected from customers or clients.[13] The theory of "third party beneficiaries" is also used to widen the net of potential parties in data breach suits. In such claims, those without a direct contractual relationship with an entity that suffered a data breach will seek to enforce the terms of a company's contract with someone else to safeguard information. The hurdle for such claims is that the plaintiff must establish that the contracting parties intended to actually benefit the plaintiffs.

Damages in breach of contract claims for data loss cases are often problematic for plaintiffs to prove, but courts are becoming increasingly open to allowing such suits for remote or unknown damages. The reason for this difficulty is that many plaintiffs in data breach cases have not experienced any actual misuse/fraud from the breach. Accordingly, for those Plaintiffs where the pilfered information has not actually been used, the argument is that they are at an increased risk of future harm. (i.e. that their information will be used in the future against their business interests or to commit future fraud

and theft). Where data or trade secret information is lost, the hurdle is lower for a plaintiff who can show his intellectual property is being used in the marketplace.

Tort-based theories of liability in data breach cases usually center around negligence and/or negligent misrepresentation claims. Under such claims plaintiffs generally allege that the breached defendant had a duty to exercise reasonable care in protecting the plaintiffs' personal information, but breached that duty by failing to establish adequate protocols or by failing to provide timely notification of the breach. In such claims the plaintiff must demonstrate: a) the existence of a duty to exercise due care; b) breach of that duty; c) causation; and d) damages.

As set forth in more detail below, plaintiffs will face the same requirements to show recognizable injury and causation, but must also show that the defendant owed them a duty of care. When negligent and/or intentional misrepresentation is included in a claim the plaintiff must prove: a) that a material misrepresentation existed; b) it was made with negligence (without reasonable grounds that it was true); c) that the plaintiff relied on the statement(s) and; d) that as a result plaintiff suffered injury.

For tort claims, a usual defense that is raised relates to the economic loss doctrine, which seeks to prevent a purchaser of a product or service from recovering in tort for economic losses where no additional damage to person or property exists. The economic loss doctrine requires such plaintiffs generally to maintain the action on a contract theory alone. Although often effective, each state's laws on economic loss doctrine vary, and many states have seen an erosion by the court's of the economic loss doctrine's application.

WHAT TO DO BEFORE AND AFTER A BREACH

A. Insurance-Before

Faced with the daunting numbers of data breach incidents and increased liability under federal and state law, as well as through civil lawsuit exposure, the insurance industry has responded with numerous products to insure against the increased risk . It was recently reported that one in three companies now has insurance designed to protect against data breaches. Marsh LLC, a New York insurance brokerage firm, recently noted that cyber insurance policies sold to retailers, hospitals, banks, and businesses rose 20 percent over the last year.[14] Such insurance is designed to fill the holes in coverage that may exist in traditional commercial policies. Initially, such policies were designed to protect against data loss and exposure of personally identifiable information, but have grown to include loss of trade secret material and other confidential data.

Last year, Target Chief Financial Officer John Mulligan disclosed that the high-profile 2013 data breach of the retail giant cost Target $61 million in out-of-pocket expenses during the fourth quarter, of which $44 million was covered by insurance. Thus, although costly, insurance was able to alleviate the devastating costs of the cyber breach to the company's bottom line.

Both first-party and third-party coverage is generally available in the marketplace. First-party coverage relates to costs resulting from the insured's actions as a result of the breach (i.e. costs for hiring professionals to assist in the investigation and response; attorney fees to advise on notification and other legal requirements; crisis management firms; computer forensics firms, etc.). Third-party coverage is designed to indemnify liability to third parties allegedly resulting from a covered claim. Such cyber-risk policies are generally available only on a claims-made basis. In a claims-made policy, coverage is triggered

when a claim is made against the policyholder during the policy period. This is important as it often takes significant time to realize a cyber breach has taken place. Thus, a new policy may well apply to a new claim that is based on a breach which occurred before the policy inception. An analysis of your business operations and potential liabilities should be the first order of business with your attorneys and insurance agent to secure the appropriate insurance coverage.

B. Notice-After

After a breach has been detected, the first thing that must be done is provide notice. This notice should be given to the following entities, depending on applicable state and federal law: 1) state and federal regulators or agencies responsible for monitoring applicable cyber material and breaches; 2) the customers and consumers whose information is subject to the breach; and lastly 3.) your insurers. After a data breach, especially one involving the disclosure of "personal information," notice to regulators, law enforcement and affected individuals is often required by statute or rulemaking as discussed above. Business entities responding to a network/privacy breach must additionally act in compliance with contractual notice obligations. This notice may be mandated to be given to the clients or customers of the corporation in specific times and manner based upon an agreement or contract the corporation suffering the breach has with its clients or customers. Moreover, the policies of insurance the corporation has covering such breaches likely has specific notice requirements. Every cyber risk policy contains a section describing the insured's duties in the event of a claim or loss, and when and how notice of a loss must be provided to the insurer is set forth in the policy. As network and privacy liability policies often include provisions of both first-party and third-party insurance, the insured's duty to give notice may depend on the type of exposure at issue. When the breach arises, you should immediately seek a quick consultation with your outside counsel who is familiar with your policies, to meet the requirements of notification set forth in the policy.

C. Defenses

It is an old saying, but a true saying: The best defense is a strong offense. In the data breach liability world, this means that having a robust plan and procedures in place to prevent a data breach will be central to showing that your company met the standard of care in doing everything it could to protect the data in its possession. Similarly, compliance with state and federal notice requirements, as set forth above, will alleviate the specter of state or federal liability on top of civil liability.

One of the major threats in a cyber breach case is a class action claim. The proliferation of cyber security data breaches has mirrored an increase in class action data breach litigation. Most class actions filed after a data breach occurs seek injuries for increased risk of "identity theft", fraudulent financial charges on credit cards, and costs incurred from having to enroll in third-party credit-monitoring services. However, not every data breach results in an injury. Accordingly, the major defense to any data breach claim is that the claimant does not have standing as no impact or real injury has occurred. Case law supports that this can be a significant hurdle to plaintiffs' claims against you and your company, and an invaluable defense.

Standing derives from Article III of the U.S. Constitution, which limits the powers of the federal judiciary to the resolution of "cases" and "controversies." U.S. Const. Art. III, §2. A plaintiff must plead and ultimately prove that he or she has suffered sufficient injury to satisfy the "case or controversy" requirement. A plaintiff must allege at the pleading stage: (1) an injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that the injury can be remedied by a favorable ruling. If the plaintiff cannot satisfy this, the claim must be dismissed.[15]

Although businesses operating in today's world face increased threats and liabilities related to a data breach, those businesses which partner with a strong and knowledgeable law firm that is well versed in cyber law and data breach claims are ready for today's challenges and opportunities. Your outside counsel should work not only with your business on risk management and claim avoidance, but also with your computer technology professionals and personnel to successfully navigate the dangerous waters of today's business environment where a data breach is a constant and continual threat.

1 See Prepared Remarks of Robert S. Mueller, Director, FBI, RSA Cyber Security Conference (Mar. 1, 2012), http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-worldoutsmarting-terrorists-hackers-and-spies

2 See, Office of Personnel Management - Special Announcement. Information About the Recent Cybersecurity Incidents; Updated June 23, 2015. https//www.opm.gov/…/a…

3 The New York Times, Feb. 5, 2015 "9 Recent Cyber Attacks Against Big Businesses" by Kevin Granville. http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0

4 The Insurance Journal. May 7, 2014. "Company Data Breach Now Costs $3.5M on Average: Ponemon Study."

5 Dep't of Defense, Strategy for Operating in Cyberspace, at 4 (July 2011), available at http://www.defense.gov/news/d20110714cyber.pdf.

6 Compiled from: 2014 Cost of Data Breach Study: Global Analysis Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC May 2014 http://www.935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf and California Data Breach Report October 2014; Kamala D. Harris, Attorney General California Department of Justice https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf

7 15 U.S. Code § 6801

8 HHS press release, May 7, 2014. "Data breach results in $4.8 million HIPAA settlements." http://www.hhs.gov/news/press/2014pres/05/20140507b.html

9 Securities and Exchange Commission. CF Disclosure Guidance: Topic No. 2 October 13, 2011. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

10 Federal Trade Commission 2014 Privacy and Data Security Update. January 2014-December 2014. https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

11 Best Practices for Victim Response and Reporting of Cyber Incidents Version 1.0 (April 2015) . http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

12 National Conference of State Legislatures Report June 11, 2015. "Security Breach Notification Laws." http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

13 In re Hannaford Bros., 613 F.Supp.2d 108 (D. Me. 2009), where the court held:
The district court correctly concluded that a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use the credit card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information. In re Hannaford, 613 F.Supp.2d at 119. When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract. In re Hannaford Bros., 613 F. Supp.2d at 119

14 The Boston Globe. "More firms buying insurance for data breaches Companies seek added protection" By Deirdre Fernandes FEBRUARY 17, 2014 https://www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html

15 See, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).; Vides v. Advocate Health & Hosps. Corp., No. 13-CH-2701 (Ill. 19th Judicial Cir. May 27, 2014).

Wayne M. Alder is a shareholder in the Business Litigation practice of law firm Becker & Poliakoff, where he focuses his practice on complex commercial litigation. He may be reached at walder@bplegal.com.