

# **Data Breach: Overview of Trends in Litigation and an Approach to Practical Prevention**

*by*

Todd B. Ruback, Esq. and CIPP

and

Albert Raymond, Chief Privacy Officer, CIPP and CISSP

September 12, 2009

## **Purpose**

The purpose of this paper is to review the topic of data breach from two perspectives: first, an overview of the trends in data breach litigation, and second, a more granular perspective of practical data protection processes that may serve as a guidepost to help reduce the risk of likelihood of data breach. Taken together the reader will understand why a measured approach to data protection can reduce the risk of financial liability from a data breach lawsuit.

## **Overview of Trends in Data Breach Litigation**

Data breach litigation is a relatively young area of law, but is growing up fast. There are numerous ways for a data breach to occur. Some of these ways include breach from external sources such as hackers breaking into your technology systems, while other ways may include disgruntled employees stealing data, or wrongfully looking at personal information that they should not have access to. Other examples of potential data breach include improper or sloppy destruction of records, as well as wrongful access to personal information by third party vendors. Regardless of the form of the data breach, lawsuits from data breaches contain significant risk to companies and this risk needs to be analyzed and appropriate controls put in place. To date the most extreme examples of financial risk from data breach litigation include the TJX case, which settled for well over \$40M and Heartland Payment Systems, which is in litigation presently and has cost to date over \$12M in initial attorney fees and other costs.

Data breach litigation has traditionally been brought in the Federal Courts as class action law suits. However, there is also significant risk of suit for data breach on state court level as well as private causes of action. Further, in many cases of data breach there may be governmental entities with enforcement powers over the company. Examples of these entities may include the Federal Trade Commission (FTC) and various states Attorneys General. Often these regulatory bodies can bring actions against the company for unfair or deceptive trade practices, which may result in substantial fines and/or penalties. In essence, a company may pay three times for the same data breach: once in the class action suit, once to the FTC and also to the states Attorney General. Such was the case with TJX.

Data breach lawsuits in the private sector have historically been based upon a tort theory of negligence.

Under a negligence approach in order to be successful, a plaintiff has to establish the following elements: 1. The defendant company whose data was breached had a duty or an obligation to protect the data, 2. The company breached that duty, or failed to meet the standard of care to protect the data, and, 3. Actual damages were proximately or directly caused by the breach of duty. Further and as a general rule of law, if the company's breach of duty was so great, or was so willful or grossly negligent to shock the public's conscience, then punitive damages may be awarded. Litigation under the negligence approach deserves thoughtful consideration for numerous reasons; chief among them is that many current data breach insurance policies have exclusions for punitive damages awards. Put into financial terms, if your company has a duty to protect information and

fails to do so to such a degree that punitive damages are deemed appropriate, the payment of such punitive damages may impact the company's bottom line since the company will be paying for them out of pocket. Further, many insurance policies also exclude regulatory fines from coverage, which means that if the FTC or states Attorney Generals join in litigation, often for unfair or deceptive trade practices, then any fines or penalties from the enforcement actions will not be covered by the insurance carrier. Often these fines and penalties can be substantial.

Although there have been some notable financial settlements in data breach litigation, the trend in the US courts has been to require that plaintiffs, in order to prevail, must establish and prove all three elements of a negligence action mentioned above. Establishing all three elements of a negligence case in data breach litigation has often been difficult due for a few reasons. First, there is not a commercially objective security standard that companies can implement in order to protect personal information. This means that courts cannot yet point to a certain set of security criteria and measure a company against it. This, however, is quickly changing in a few areas. Healthcare now has an objective security standard established by HIPAA, which was recently expanded through the HITECH Act. The amended HIPAA now applies to not only healthcare providers and insurers, but also to Business Associates, which are vendor in the healthcare industry that support the covered entities. This means that vendors who have access to personal information in the health care industry must soon have in place technology and security systems that are objectively HIPAA compliant. Potential liability under the new HITECH Act for not being HIPAA compliant includes increased civil fines of up to \$1,500,000 per violation, more aggressive enforcement by the Department of Health and Human Services, new enforcement risk at the state level through the states Attorney General, including state level fines, and for cases of willful neglect, potential criminal liability for key executives.

For non-healthcare related industries there still generally remains a subjective standard of care of reasonableness and appropriateness that the courts default to. This too may be changing quickly. The payment card industry, led by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc., created the Payment Card Industry (PCI) Security Standards Council, which established the Data Security Standard (DSS) to encourage and enhance cardholder data security and facilitate the adoption of consistent and objective data security measures globally. An emerging trend is that states are now looking at the objective PCI-DSS security standard as a replacement for the subjective reasonable and appropriate standard of care. At least two states (Minnesota and Texas) either have or are considering enacting their state laws to make the PCI-DSS a mandatory security standard for all companies doing business in those states. Many other states are in early stage discussions on the same issue. From a litigation perspective this means that plaintiffs will be able to point to an objective set of security measures, procedures and protocols as the standard of care that a company was supposed use in order to protect personal information against a breach. Thoughtful consideration needs to be given to this issue by a company because PCI-DSS compliance is expensive and is not a one-time event, but rather is an ongoing process that requires an ongoing investment and commitment across the entire enterprise. If the PCI-DSS security

standard becomes the legislated standard for most states, then the plaintiffs will have an easier path to money awards since they may be able to discover any weaknesses in a company's compliance processes as proof positive of a breach of a standard of care.

Presently if a plaintiff can get past the step of establishing that a standard of care for protecting personal information existed and that the defendant failed to meet that standard of care, he/she must still prove that actual damages were incurred as a proximate or a direct result of that failure. This last element of a traditional negligence suit has been difficult for plaintiffs to prove in data breach litigation. However, there appears to be some glimmers of hope for plaintiffs. In *Piscotta v. Old Nat. Bancorp* (2007) the Court held that a plaintiff need only prove the threat of a future harm or show that the defendant's act increased his risk of future harm in order to prevail on the damages element. But generally most courts have held that actual damages proximately caused by the defendant must be established in order for the plaintiff to prevail. (See, *In Re Hannaford Bros. Co.*, 2008 U.S Dist. LEXIS 46545).

Notwithstanding the present proof requirements, there have been instances of substantial settlements by defendants in data breach litigation. The decision to settle a data breach law suit is often based on many factors, some of which may include a risk assessment of cost of suit, the likelihood of an unfavorable outcome, the fear of uncertainty and how it would impact the company's stock price, the risk of loss of business and/or the loss of reputation and goodwill, which is a booked asset, and insurance carriers pressing for settlement. Many of these factors that impact a decision to settle a data breach lawsuit are exclusive of whether or not a plaintiff incurred actual harm. For example, in 2007 the Veteran's Administration chose to settle class action litigation based upon an employee taking a laptop home that contained information of millions of present and former veterans. The laptop was stolen and then later recovered by the FBI, which conclusively determined that no personal information on any veterans was taken. The case was settled for \$20M. Another case of interest is *TD Ameritrade* (2009), in which an employee mistakenly threw files with personal information about clients in the dumpster behind the building. The Court approved a settlement for \$1.9M although it found that the plaintiff could not prove actual damages.

~

This second, complementary section of the paper deals with the repercussions of dealing with the breach, and the proactive steps a company may take to prevent the kinds of breaches that have plagued many public and private companies lately.

## **Incident Response – *General Steps***

An excellent first step in the incident response process is for a company to simply define and understand what the terms ‘violation’, ‘incident’ or ‘breach’ mean in the context of its industry’s lexicon. (We’ll use the term ‘incident’ here as the all-purpose generic term that means something that happens to your company or customers that is not a pleasant or welcome event). They may already be defined by your federal or state regulators, or other laws that govern your industry or company. If so, you should align your understanding of an incident to these already defined measures, as you will probably be legally held to them in the case of a breach or incident.

### **‘Incident’ Defined**

Here is a good example of what might reasonably be called an ‘incident’ and will require you to have a response prepared for:

“Incidents are understood and defined as an attempted or actual unauthorized disclosure of (or access to) any non-public personally identifiable information (NPI) or personal health information (PHI) relating to an identified individual, including our clients and employees. Incidents can occur within our company, on our employee home equipment, at vendor or consultant locations.”

Based on your company’s tolerance of risk (or for litigation) you can then decide if, when, and how to respond because you now have defined the parameters of what is actionable by you.

Second, you should as a company define, document and publish incident procedures that are to be followed in the event of an incident. The procedure should be a ‘who does what and when’ delineation of steps to react to the incident. The procedures need not necessarily be overly detailed or verbose, but they should not be subjective or too generic as to invite indecision or confusion during a time when you least want it. Refrain from broad statements like “Illegal activity should be reported.” Rather, you should include pointed wording and closed-end phrases like “Any confirmed illegal or suspicious activity on the production floor should be escalated immediately to the Vice President of Operations.”

For these scenarios, it is important to have single focal point of accountability to report incidents to. Even if that person delegates or designates a team to handle the follow up, at least the response has an owner. Notifying a group of people may get you the same result when you send a question to a group of people on an e-mail message: everyone thinks it is addressed to someone else, and no one ends up answering.

Once a central point of internal contract is appointed, then a real or virtual or real response team can be created. Depending on the size of your company this may be an army of one (an army of one is still an army, after all), or a group of 25 people. If you don’t have the luxury of resources that can be dedicated full-time to incident response, then a virtual team can be named that comes together in a time of crisis to deal with the incident, and then just as quickly dissolve once the storm has passed. This process allows

a company to harness the particular expertise of its employees but still allows them to do their day jobs.

To keep everyone on this team in the loop on updates during the incident handling process, a distribution list should be created with only these team members on it (Call it, “Incident Response Task Force”, for example). Setting up a defined and restricted list like this allows all communications to stay within bounds and prevents secondary conversation threads from occurring. It also allows for easier searching, storage and retrieval for ‘lessons learned’ meeting later.

Finally, to keep other parties or entities up to date on the progress of the handling of the incident, you should also define a central point of contact for external parties (clients, customers, regulators, senior management). This person can be the face or spokesman for the team so the status messages from the team are concise and owned by an accountable party.

### **Incident Response – *Specific Steps***

Once you set up the framework for general steps to take to address incidents, you should drill down towards more specific prevention and reaction measures. The following steps are typically what you should or must do as defined by the various existing state privacy and/or breach notifications. Since there is currently no Federal law superseding all the various state iterations, you should be intimately familiar with all of the laws or at least the most stringent one in states where your company does business. In some states, for example, you must notify the State Police or state Attorney General when there is a security breach that is determined to adversely impact a resident of that state. It does not make sense to notify every AG in every or any state that you have a breach, but you should review every state specific breach you experience and have a ‘cheat sheet’ matrix of the states that require some specific action beyond simply notifying the affected consumers.

Communication of an incident to a consumer should be a well-written, well-thought out message. No individual wants to receive a notice of their financial crown jewels being lost, stolen or compromised and then *still* have no idea what has really happened to their data. At the very least your message to the consumer should be that ‘though we did not prevent what happened, we know what happened and what to make you aware of it, and make you whole again’ (if applicable). Your communication letter should be a paragon of decisive, straightforward language free of industry jargon or legalese designed to obfuscate or give the company a loophole out of any liability.

Each and every letter should be, to the most reasonable extent possible, customized to the recipient. Nothing irritates a reader more than the heading ‘Dear Valued Customer.’ (Really? If I am so valued then why didn’t you even go to the trouble of getting my name on this letter?!?) If ten million records are lost, stolen or compromised, it may be cost prohibitive to get an individuals name on every letter, but if you experience one-off breaches or incidents like lost packages or letters, then a customized letter to the

individual marks your company as one in touch with its customers - a not invaluable trait to have especially in light of an unpleasant experience that the customer has just realized.

Regarding the topic of making customers whole due to a breach or incident either by your company or by a third party that your company has hired or contracted with, the prevailing wisdom is that you should err on the side of caution and make some kind of credit monitoring available to the customer. Regardless of the responsible party, you cannot defer fault to someone else and not expect the taint of culpability to remain with your company. Blaming the post office for a lost package might be convenient, but it is a less than honorable approach to customer service. At the least, you can take the blame – even disclose the true nature of the cause of the incident, but **you** should be the one to assist your customer. You can always subrogate the other party later to recover any costs that you believe should fairly be absorbed by them.

Finally, in order to get a sense of the patterns and frequencies of your incidents, you should track and document the historical record and frequency of the incidents. Ideally, you should also track the root cause of the incident and the responsible party who caused it. Some example of categories and root causes are outlined below, but the primary intent here is to get your company to be able to quantify this experience. What is not tracked or measured cannot be improved. Having these metrics allows the company to identify pervasive issues that are out of its control to resolve, and more importantly, ultimately be able to identify the tangible issues that it can remediate.

## **Incidents In The Real World**

To better help your Incident Response team deal with scenarios that may arise in your line of business or vertical, it is helpful to try and articulate the possible scenarios that may most occur in your line of work. While you cannot possibly define every likely incident (and you not should try this exercise in futility either), you should be able to imagine a short list of the ones within the realm of possibility. For example, if you are in the financial service sector or some other industry that collects and retains sensitive customer data, your list of possibilities may read like this:

*Possible scenarios for privacy or security incidents are:*

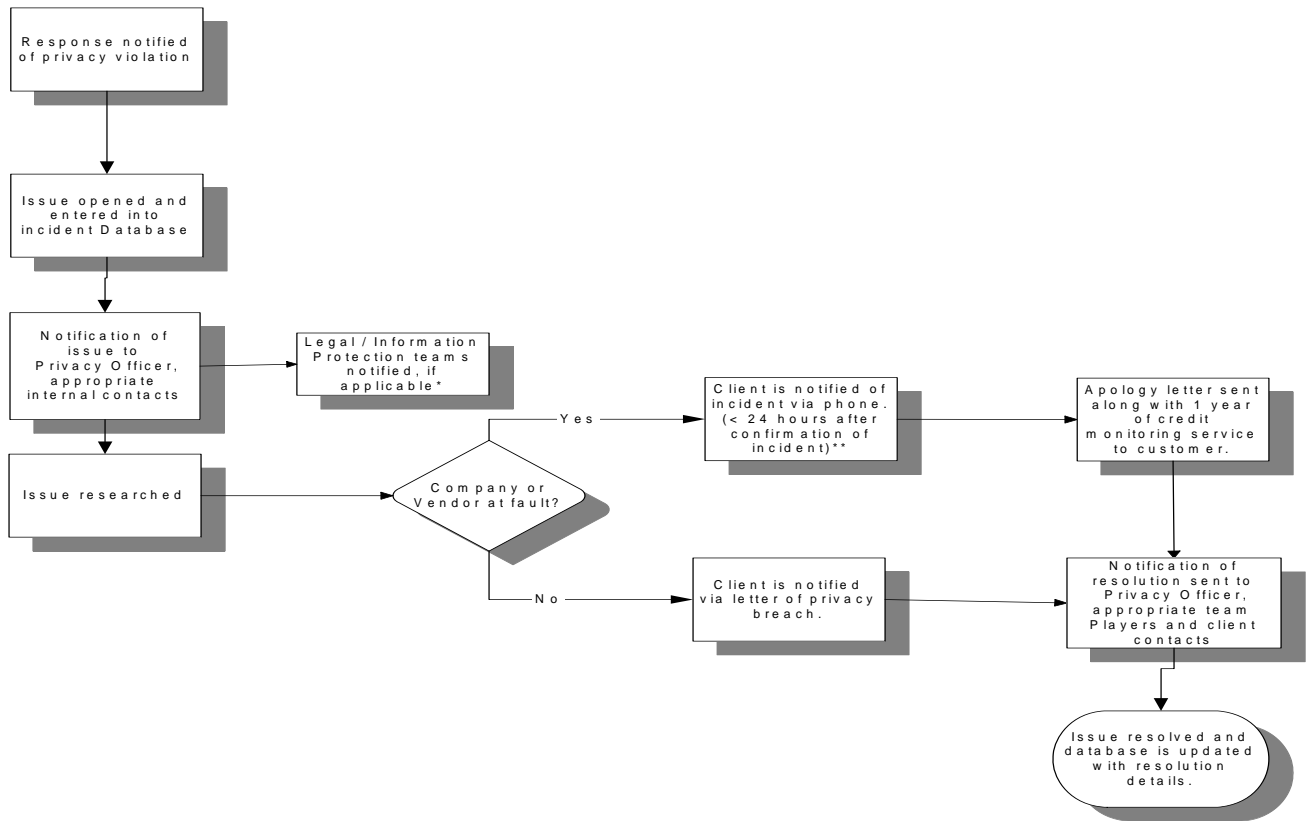
- A customer calls indicating that their privacy or identity may have been compromised (e.g. suspicion of identity theft, or phishing scheme);
- System breaches/intrusions (e.g. hackers);
- Theft of physical equipment containing sensitive information;
- Break-ins or theft at company physical locations or your vendors/service providers;
- Unauthorized access to data centers;
- Breach of data streams between your company and third parties;
- Missing documents or unauthorized access to documents;
- Unauthorized access to email;

- Incidents occurring with non-company hardware (home personal computer, phone, personal email address, etc. – relevant to Tele-Commuters);
- Data transfers of sensitive information that is either unencrypted or not transmitted over secure connections (including e-mail).

Once you have attempted to articulate a list of possible and most likely scenarios that may impact your company, you should then try and flow out the incident response in a Visio diagram to help everyone involved visualize the process. For the right-brained people of the world, this exercise may also help flush out any loose ends or less than obvious gaps in your response process.

Here is an example of a diagrammed process by roles:

### Incident Response Process



Here are examples of specific categories and tracking fields

<b>Root Cause</b>	<b>Responsible Party</b>
Address Label Error	Service Provider
Data Entry	Client
Delivered to Wrong Address	Process – Internal
Privacy Violated Verbally	Uncontrollable – Internal
Intermingled Package	Consultant
System error/issue	Customer
Delivered to correct address/Package not received	Delivery Carrier Employee - unintentional Mailroom Employee - intentional Malicious External (e.g. hacker, worm)

## **Prevention and Remediation**

Ideally, the best (and usually cheapest) medicine is prevention. Prevention of incidents can best be effected, at least by your employees, with an easy four step process:

- Awareness
- Awareness
- Training
- Awareness

You may have noticed the repetition of ‘awareness’ on the list. It is not us just being flip when we assert that a predominately large percentage of issues occur due to circumstances that could have otherwise been controllable had the proper internal processes, procedures or levels of awareness been in place. At this point in the security prevention lifecycle, most mature companies are aware of the minimum controls that they must have in place to be viable (‘commercially reasonable’ is the term usually seen in contracts) and be in compliance with most regulation and security standards. For most of us, the perimeter is already secured with locks, guards, firewalls, Dobermans, a moat, etc. It is the malicious or trusted insider who has the most impact on the volume of incidents. That is why your prevention efforts and monies should be focused on the most likely risks to your data, customer information or intellectual property’s safety. This approach is the most judicious course you can take when it comes to preventing an event that you don’t want to read on the cover of the Wall Street Journal.

Here are some sample procedures and guidelines which unequivocally state what a company’s policies are in a number of threat vectors that can otherwise result in data leakage, compromise or exposure if not handled correctly:

- 
- **Email Guidelines**
- Employees should not send more than one piece of customer personal information such as NPI or PHI in an email (*e.g. sending name **and** SS Number*)
- Employees should delete portions of emails that contain personal information when replying to an email
- Employees should use the e-mail encryption service when sending e-mails with PII or PHI contained in them is an absolute necessity
  
- **Telephone Guidelines**
- Be cautious when revealing information to individuals, especially at a distance
- Verify identity (Ask questions only a real customer would know)
- Verify that customer has granted consent to disclose information to a third party
- Be aware of who is around you when discussing sensitive information
- Perform a call back if necessary
  
- **Handling Hardcopy**
- Practice the ‘clean desk’ policy; don’t leave sensitive information lying about on the desk
- Put documents that are being worked on in folders and lock them away if you must leave your desk
- Shred sensitive information that the company does not need to retain
- When using printers and copiers, be sure to remove all sensitive information
  
- **Vendor and Supplier Guidelines**
- Be aware of how vendors and suppliers are securing information and protecting customer privacy
- Make sure language is included to enforce compliance in all contracts
- All contracts must be approved by Legal counsel and Information Protection team
- Steer clear of vendors that do not have secure practices
  
- **Technological Controls Already In Place**
- User ID & Password Requirements
- Network Security- Firewalls and Intrusion Detection
- File and application security
- Limited Employee administrative access to personal computers
- Disallowing CD/DVD Burners
- Disabling the use of a USB Port

## **Conclusion**

In this age of the free flow of information, your customers and clients do not realistically expect you to *never* have a security or privacy breach. No rationale person can expect all of their data in all its iterations in all of the locations that it is dispersed to forever remain safe and secure. It is the trade-off we (at least in America) have agreed to for

convenience, service and freedom. What those customers and clients *do* expect you to do is have a process in place to reasonably prevent the incident from happening, and when it does happen, have a plan in place to deal with the consequences. Part of those consequences involve notice to the client/customer of what happened, details on how you will make the client/customer whole again, and finally, the plans to ensure that this same event does not happen to them again.

As we referenced earlier in the emphasis on training of employees, rather than trying to avert security or privacy incidents via threats, coercion or punishments, real, effective and long-lasting prevention is best instituted as part of a company culture. Only by engaging the employees and attempting to get them invested in the process, can you then effect a viable strategy for both preventing incidents, and mitigating them to acceptable risks levels if they happen. When the confidentiality and protection of your customer's data, your intellectual property or trade secrets are deemed to be part of everyone's day job – and not just the InfoSec team's problem – will your company be able to get comfortable that the prevention and possible remediation of the inevitable incident will be handled professionally and expeditiously.

#### About the Authors:

Todd B. Ruback is an attorney and a Certified Information Privacy Professional (CIPP) at the law firm of DiFrancesco, Bateman, Coley, Yospin, Kunzman, Davis & Lehrer, P.C. He is chair of the law firm's Privacy and Technology law practice. He can be reached by email at [Truback@newjerseylaw.net](mailto:Truback@newjerseylaw.net) or by telephone at 908-757-7800.

Albert Raymond is the Chief Privacy Officer at PHH Mortgage and is also a Certified Information Privacy Professional (CIPP) and a Certified Information Systems Security Professional (CISSP). He can be reached at [albert.raymond@phhmortgage.com](mailto:albert.raymond@phhmortgage.com). Mr. Raymond's blog is found at <http://privacynsecurity.blogspot.com/>