

# **The Legal Risks of Data Loss in the United States**

A Bcrypt White Paper

Written by Robinson & Cole LLP

## Executive Summary: Data Loss in the U.S.

Historically, in the U.S., companies have treated their customers' names, ages, purchases, addresses, social security numbers and other personal information as valuable corporate assets to be collected, used and in some cases sold, often without the knowledge of the individuals who provided such information. With few exceptions, the government had no role in regulating or restricting this activity.

With the advent of the Internet, personal information became far easier to collect, aggregate, sort and share. With this ease came increasing concerns about the use, misuse and security of information, leaving companies and individuals vulnerable to exposing valuable data. In response, Congress and various states adopted a patchwork of legislation to regulate the collection and security of certain classes of personal data, whether in paper or electronic form, considered to be particularly sensitive.

However, to date, no generally applicable federal law has been enacted specifically regulating the collection, use and sharing of an individual's personal information. Rather, the Federal Trade Commission (FTC) has promoted industry self-regulation, based on statements of fair data collection and security practices, including adopting a privacy policy that provides consumers with information on a company's data practices, as well as what measures they are taking to secure private data from unauthorized access and accidental disclosure.

The focus on data security has intensified in the U.S. during the last three years, due largely to widespread publicity over massive security breaches. Following California, an overwhelming majority of states have enacted legislation requiring notification of breaches that involve personal information.<sup>1</sup> Massachusetts is a prime example as it prepares to implement arguably the most stringent state data protection law in the country in January 2010.

The state-level data breach notification laws have also helped to build awareness around the specific cost of data loss. In early 2009, the *U.S. Cost of a Data Breach Study*, released by the Ponemon Institute, revealed that cases involving compromised data cost U.S. companies an average of \$202 per customer record in 2008, compared to \$197 in 2007, representing nearly a 40 percent increase since 2005. The average cost of a data breach in 2008 was \$6.65 million.<sup>2</sup> Though staggering, that cost could easily be avoided by implementing correct security measures.

This white paper, commissioned by Becrypt and written by Robinson & Cole LLP, explores the many risks associated with losing data and other valuable and confidential information, presents an overview of relevant U.S. legislation, and offers suggested possible best practices and guidance for companies to protect against data theft and loss.

---

<sup>1</sup> <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

<sup>2</sup> "Costs of a Data Breach – Can you Afford \$6.65 Million?" Dr. Larry Ponemon, February 4, 2009, [http://www.cio.com/article/479101/Costs\\_of\\_a\\_Data\\_Breach\\_Can\\_You\\_Afford\\_.Million\\_](http://www.cio.com/article/479101/Costs_of_a_Data_Breach_Can_You_Afford_.Million_).

## Data Loss Risks

The most detrimental cost to a company affected by a data breach is the potential loss of customers, revenue and share value, not to mention the embarrassment and public relations nightmare associated with such an incident. The specific risks, however, vary depending on the type of company or the nature of the data involved. Some of the most common ways in which data is lost include network hacking; insecure wireless networks; lost or stolen laptops and portable devices; media lost in transit; unredacted online records; breaches in physical security; phishing or pretexting scams; botched software upgrades/updates; insecure disposal of print and electronic media; human error; rogue or disgruntled employees; misdirected mail and faxes; malicious software; and/or failings by vendors and service providers. Surprisingly, a recent study by Verizon found that 74 percent of data breaches investigated were caused by external sources, 32 percent were linked to business partners and only 20 percent were caused by insiders - a finding that may be contrary to certain widely-held beliefs.

The extent of these risks is highlighted by the growing number of data breaches and the legal cases that often result from them. Regardless, data breaches can have an enormous impact on a company's finances and reputation.

The monetary cost of a security breach can be extremely high. In addition to the figures discussed above outlining the cost of a data breach, another recent Ponemon study<sup>3</sup> estimated that every lost laptop can cost companies up to \$200,000, with an average cost of \$49,246. Among other things, those incurred costs include internal investigations, forensic experts, consumer notification, crisis management, call centers, credit monitoring, attorney fees, payment card industry fines, creating and disseminating software patches, litigation expenses, subpoenas or other government action by state Attorneys General or by the Federal Trade Commission, stock price, reputation, trust, technology upgrades, and even the loss of the ability to process credit cards.

Given the sensitive nature of information they work with, financial institutions and health care providers are generally exposed to the greatest amount of risk. Whether the breach involves unauthorized access into a company's systems by an employee or remote intruder, or occurs because of a loss or theft of physical property, such as a laptop or disk, it almost always makes news headlines and affects the company negatively. Some recent examples include:

- Continental Airlines reported in January 2009 that a laptop containing records used for security background checks was stolen. The laptop, which had been in a locked office in New Jersey at the time of the theft, contained the individual names, addresses, Social Security numbers and fingerprints of more than 200 individuals. The reports do not indicate that the laptop or the records were

---

<sup>3</sup> "Lost Laptop Can Cost A Company \$49,246: Study," Michele Masterson, April 23, 2009, ChannelWeb, <http://www.crn.com/security/217100086;jsessionid=5MTST0AFDUR2AQSNDLRSKHOCJUNN2JVN>

encrypted. Also in January 2009, Heartland Payment Systems, one of the nation's largest credit card payment processors, announced what may have been the largest data breach in U.S. history. The company learned of the breach after Visa and MasterCard notified it of suspicious activity surrounding processed card transactions. The company determined that intruders had hacked into Heartland's computer system and accessed data that was not encrypted properly. The exact number of victims remains unknown, but the potential is exceedingly high – Heartland processes 100 million payment card transactions per month for more than 175,000 merchants.<sup>4</sup> Heartland has since been sued for damages and relief stemming from the delay in notifying its customers.

- In April, 2009, the State of Oklahoma Department of Human Services experienced the theft of a laptop from the car of an agency employee. More than one million residents' names, addresses, home phone numbers and Social Security numbers were stored, unencrypted, on the laptop.<sup>5</sup>
- In 2007, TJX, the parent of leading off-price home and apparel retail stores such as TJ Maxx and Marshalls, reported that on multiple occasions dating back to 2005, hackers had gained access to approximately 45.7 million unencrypted credit and debit card numbers. The investigation revealed that a financial fraud ring exploited the company's outdated encryption systems to access financial data being transmitted between hand-held price-checking devices, cash registers and the store's computers. Officials have made more than 11 arrests globally in connection with this breach, with at least one conviction.<sup>6</sup> To date, company and external estimates on the cost of the breach range from \$256 million to \$500 million to \$1 billion. Some 20 class actions brought by individuals, card issuing banks, state banking associations and shareholders were eventually settled out of court. The retailer is still defending claims brought by two financial institutions. There were also investigations by federal and several state enforcement agencies.
- In October 2008, an Ohio medical insurer reported the loss of 11 disks containing personal information of 36,000 employees and retirees. The disks were mailed from the insurer's office to the plan office, both in Columbus. Apparently, because the disks were mailed without sufficient postage on the envelopes, they did not arrive at their destination and remain missing, perhaps within the postal system.

Not only is a company at risk of data loss relating to its customers' sensitive personal information, but also its employees' confidential information. For example, in July 2008, the Washington Metropolitan Area Transit Authority accidentally published its employees' Social

---

<sup>4</sup> "Hackers breach Heartland Payment credit card system," January 23, 2009,

[http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach\\_N.htm](http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm).

<sup>5</sup> "Unencrypted laptop with 1 million SSNs stolen from state," SC Magazine, <http://www.scmagazineus.com/Unencrypted-laptop-with-1-million-SSNs-stolen-from-state/article/131333/>

<sup>6</sup> "A Chronology of Data Breaches," Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>.

Security Numbers on its website.<sup>7</sup> While a company may not suffer the same level of embarrassment or scrutiny it would upon losing customer data, the employees' trust in the organization may be lost, and, worse yet, the company may be held financially liable to the employee.

Company carelessness can also lead to avoidable data loss. In 2005, a disgruntled former Kaiser Permanente employee posted links on her personal blog to a Kaiser document posted on a public website, claiming to expose the company's breach of HIPAA. The document, entitled "systems diagram," included database names, IP addresses, computer codes and screen shots, potentially affecting some 140 Kaiser insureds. The company later sued the former employee and obtained an order to destroy any company information in her possession and enjoining her from using or sharing the information. However, as a result of the company's failure to protect this information from disclosure, Kaiser Permanente was eventually fined \$200,000 by the California Department of Managed Healthcare.<sup>8</sup>

### **Relevant Legislation and Industry Self-Regulation**

The impact data loss has had and continues to have on U.S. citizens has resulted in a wide variety of data security-related legislation at both the federal and state levels. A number of federal laws have been adopted requiring companies to take measures to protect and secure the most sensitive information, such as financial and health information, and to protect particular groups of people, such as children. The state legislation has focused more on providing notice to consumers in the event of a breach. To date, 44 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted laws requiring companies to notify individuals if their personal information has been compromised. The financial and direct marketing industries, among others, have also adopted certain self-regulatory requirements for its members.

Prominent federal and state laws and industry practices include:

#### **Federal**

- **Health Insurance Portability and Accountability Act of 1996 ("HIPAA").** Under HIPAA's Security Rule, *electronic* protected health information ("e-PHI") must be protected by administrative, technical and physical safeguards.<sup>9</sup> This includes, for example, implementing policies and procedures that address the disposal of e-PHI and/or the hardware or electronic media on which it is stored. Procedures must also be implemented to remove e-PHI from electronic media prior to the media's re-use.<sup>10</sup>

---

<sup>7</sup> See note 6.

<sup>8</sup> See note 6.

<sup>9</sup> CRS Report for Congress, "Data Security: Federal and State Laws," Gina Marie Stevens, [http://www.asisonline.org/newsroom/crisisResponse/CRS\\_report0807.pdf](http://www.asisonline.org/newsroom/crisisResponse/CRS_report0807.pdf).

<sup>10</sup> U.S. Department of Health and Human Services, "Frequently Asked Questions about the Disposal of Protected Health Information," <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf>.

Under HIPAA's Privacy Rule, covered entities are required to protect the privacy of protected health information, *regardless of its form* (i.e. electronic or otherwise) ("PHI"), including, for example, by implementing reasonable safeguards to restrict incidental and prevent prohibited uses and disclosures of such information.<sup>11</sup> The Privacy Rule also extends to the entire workforce of a covered entity and requires contractual assurances from business associates that handle PHI on an entity's behalf.<sup>12</sup>

In addition to HIPPA, new data breach notification obligations to health information were created under the American Recovery and Reinvestment Act of 2009, enacted on February 17, 2009.

- **The Gramm-Leach-Bliley Act of 1999 ("GLBA").** GLBA aims to protect the privacy and security of consumers' personal information. GLBA's Financial Privacy Rule governs the collection and disclosure of a customer's personal financial information by financial institutions and by companies who receive personal financial information.

Under the GLBA's Safeguards Rule, financial institutions (including credit reporting agencies and others that receive, but do not collect, information from their own customers) are required to design, implement and maintain security and other safeguards to protect customer information.<sup>13</sup>

- In June 2005, a new "**Disposal Rule**" went into effect under the **Fair and Accurate Credit Transactions Act of 2003 ("FACTA")**, requiring organizations that use consumer reports (i.e. consumer reporting agencies, lenders, employers, attorneys, etc.) to properly dispose of information contained in such reports and records. No explicit rule is presented; rather, organizations are instructed to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits associated thereto, and changes in technology. The crux of the rule is to protect against unauthorized access to, or use of, the information. Organizations may choose to shred papers containing such information or, if in electronic form, erase or destroy such information so that it cannot be read or reconstructed.<sup>14</sup> FACTA also requires companies to truncate credit card numbers on receipts, forbidding companies from including the credit card's expiration date or any more than the last five digits of the credit/debit card number on them. Pursuant to FACTA, regulations known as the Red Flag Rules were created by the FTC, the federal bank regulatory agencies, and the National Credit Union Administration, requiring financial institutions and creditors to

---

<sup>11</sup> *Id.*

<sup>12</sup> University of Miami, Miller School of Medicine, Privacy/Data Protection Project, "Privacy Standard/Rule," [http://privacy.med.miami.edu/glossary/xd\\_privacy\\_stds.htm](http://privacy.med.miami.edu/glossary/xd_privacy_stds.htm).

<sup>13</sup> Federal Trade Commission, Privacy Initiatives, "Financial Privacy: The Gramm-Leach-Bliley Act," <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>; see also Federal Trade Commission, "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act," <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm>.

<sup>14</sup> Federal Trade Commission, "FACTA Disposal Rule Goes into Effect June 1," June 1, 2005, <http://www.ftc.gov/opa/2005/06/disposal.shtm>.

develop and implement written identity theft prevention programs to respond to various “red flags” indicating possible identity theft.

- **The Children’s Online Privacy Protection Act of 1998 (“COPPA”)** is designed to allow parents the ability to control what information is collected while their children use the Internet, as well as how such information may be used. Generally speaking, any website directed at children younger than 13-years-old (“Children”) that collects personal information from them, or directed at a general audience while knowingly collecting such information from children, or websites with a separate kid’s area that collects such information from children, is covered by the law. Among other requirements, website operators must maintain the confidentiality, security and integrity of personal information collected from children.<sup>15</sup>

**The Federal Trade Commission Act (“FTC Act”)** prohibits unfair competition or unfair or deceptive acts or practices in or affecting commerce. If an organization’s actual data collection, use, sharing or security practices differ from its posted privacy statement, the company may be accused of engaging in unfair or deceptive trade practices, as consumers presumably rely on the privacy statement when providing their personal information to the company. Under the FTC Act, the FTC has developed and imposed security procedures on various organizations including administrative, technical and physical safeguards.<sup>16</sup> While the FTC does not require data encryption, it nevertheless recommends it as a best practice.

### **States**

- Several states have adopted **breach notification laws**, and while they vary state to state, the laws generally require a company to notify the affected individuals if a company knows or believes unencrypted personal electronic information has been accessed improperly or accessed by an authorized person. The first such breach notification law was adopted by California in 2002. Since its enactment, 43 other states have enacted similar legislation, and the California laws themselves have been revised to give consumers more specific information about the breach. Of course, over time, breach laws have evolved. In Pennsylvania, the Senate recently approved a change to the state’s breach law that would require public agencies to notify state residents of a breach of their personal information within seven days of discovery of the breach. In its current form, the law, like most state breach notification laws, simply requires notification “without unreasonable delay.”

Breach notification laws in Nevada and Massachusetts are considered the toughest to date. In Nevada, for example, any business in the state that transfers personal information of a customer through an electronic transmission (other than by facsimile) to a person outside of

---

<sup>15</sup> Federal Trade Commission, Privacy Initiatives, “Children’s Privacy: The Children’s Online Privacy Protection Act,” <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html>.

<sup>16</sup> See note 9.

the secure system of the business must use encryption to ensure the security of such transmission.

New breach notification standards are set to take effect in Massachusetts in January 2010, after the original deadline was already extended previously to May 2009. The regulations, applicable to anyone that owns, licenses, stores or maintains personal information about a Massachusetts resident, establish minimum standards to safeguard information contained in both paper and electronic records. Such persons will be required to develop, implement, maintain and monitor a comprehensive, written information security program (“WISP”) applicable to any records containing personal information. Each information security program must, for example:

- Identify and assess internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other record containing personal information;
- Impose disciplinary measures for violations of the comprehensive information security program rules;
- Prevent terminated employees from accessing records containing personal information;
- Take reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information;
- Collect the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected; retaining such information for the minimum time necessary to accomplish such purpose; and permitting access to the smallest number of persons who are reasonably required to know such information in order to accomplish such purpose;
- Regularly monitor and audit employee access to personal information; and
- Review the scope of the security measures at least annually.<sup>17</sup>

Each program must also establish and maintain a security system covering its computers, including any wireless system. Such a system may require the encryption of all transmitted records and files containing personal information, including those in wireless environments that travel across public networks.<sup>18</sup>

---

<sup>17</sup> 201 CMR 17.00, “Standards for The Protection of Personal Information of Residents of the Commonwealth,” <http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca>.

<sup>18</sup> *Id.*

## **Industry**

- The **Payment Card Industry Data Security Standard (“PCI DSS”)**, is a set of 12 basic security requirements with which all entities that process, store or transmit certain “cardholder data” must comply. While not law, the PCI DSS is an industry standard enforced and disseminated by the credit card institutions through contractual obligations imposed on their member banks that, in turn, ensure that merchants and other entities are in compliance. As part of the PCI DSS, member banks are required to encrypt certain information. If such information is not encrypted, the banks may be subject to fines by the credit card institutions. During the last several years, Congress has considered various proposals on a federal breach notification law, but none were enacted until 2009 when a provision included in the federal stimulus legislation gave the FTC the authority to adopt regulations on security breach notifications involving health records. Because the state laws are not identical, and in some cases, have significant differences, it is sometimes challenging for large companies to comply with laws in multiple states. Some would like Congress to adopt a generally applicable security breach notification law to address this issue.

## **Best Practices and Guidance**

With the growing use of the Internet and the collection, transmittal and storage of electronic records comes the increasing problem of financial and identity theft and data loss. While complete data security seems at best a moving target, there are several measures that a company can and should take to minimize the occurrence of data loss. The following practices are suggested to help companies avoid data breaches, and in the event one occurs, to be able to respond quickly:

- 1. Conduct a security risk assessment and develop a security plan and policy.** The policy should include statements addressing the points below. Once the policy is developed, training should occur for all members of the organization.
- 2. Use password protection.** Use passwords for log-in and access to sensitive data. Only unique passwords should be used as identifiers and for accounts. Avoid using information that can be easily checked, such as names, birth dates, Social Security Numbers, or phone numbers. Restrict access to email, screen savers and the like with passwords.
- 3. Use encryption to further protect sensitive information.** Make sure all sensitive information is encrypted, especially when physically or electronically transferring files with personal information, and when storing files on laptops, portable devices, DVDs, or CDs.
- 4. Physically secure sensitive information, equipment and files, and restrict access.** Sensitive data should be physically restricted in a secure location. Maintain records of who must have access to the electronic files and how the information is distributed.
- 5. Manage files and systems, including archiving and updating.** Periodically review system capacity and files for updating, deletion, or storage in secure locations. Wipe portable devices before disposing of them or transferring them to a new user. Have a routine for review and disposal of paper information that is no longer essential. Adopt and follow a retention policy.

- 6. Employ and update software to guard against viruses, spam and malware.** Use a firewall for the network. Use only secure servers. Upload and apply patches as they become available.
- 7. Adopt and follow terms of company privacy policy.**
- 8. Audit, test, and verify.** Periodically conduct audits of the system.
- 9. Monitor system use and information access.** Use application logs.
- 10. Terminate access for former employees.** Coordinate with human resources to disable passwords and access upon termination and to collect any portable devices and laptops.

## **Conclusion**

It is clear that data loss can cripple an organization – not only by the financial costs associated with it, but also by the brand degradation it causes. The massive TJX breach in Massachusetts is a prime example of just how detrimental a data breach can be. Not only has the company already spent four years dealing with the repercussions of the breach, but it has also lost millions (possibly a billion) of dollars as a result. For many companies, such costs could put them out of business.

Despite more stringent breach notification laws, businesses have to remember that such initiatives are designed to protect the individual. It is up to businesses to protect themselves, which they can easily do by implementing a comprehensive security plan as outlined above.

*This White Paper contains a general overview and statement of the law and is not a substitute for obtaining detailed legal advice. You should seek specific advice on a particular issue.*

## **About Becrypt**

Becrypt is a leading global supplier of innovative Information Assurance solutions and services, providing secure, feature rich, out of the box products, that are government-certified and suitable for all industry sectors.

Becrypt is the largest supplier of encryption technology to the UK Government, Ministry of Defence and UK Police.

Becrypt plays a leading role in the Information Assurance industry through membership and participation in the Trusted Computing Group (TCG) and the Organization for the Advancement of Structured Information Standards (OASIS) where we sit on the Key Management Interoperability Protocol (KMIP) committee. In addition, we currently chair the Crypto Developers Forum – Baseline WG (UK).

Through technology and OEM partnerships Becrypt enables third-party solutions with encryption and other data security capabilities.

Becrypt has offices in Annapolis, Maryland, USA and London, UK and Sidney, Australia serving clients worldwide.

For more information please visit: [www.Becrypt.com](http://www.Becrypt.com), email [USA@Becrypt.com](mailto:USA@Becrypt.com), or call: (800) 775 0416.

## **About Robinson & Cole's Technology & Data Security Practice**

Offering comprehensive legal and business experience in transactional, regulatory and litigation matters, our practice serves vendors of technology and technology-enabled products and services around the world. Our global reputation as a market leader in protecting the North American legal interests of software suppliers, system integrators and professional services organizations is earned from nearly 30 years of experience helping technology clients achieve their strategic, financial and operational goals while protecting their valuable intellectual property. Contact partners Kathleen M. Porter at [kporter@rc.com](mailto:kporter@rc.com) and Richard Green at [rgreen@rc.com](mailto:rgreen@rc.com). [www.rc.com](http://www.rc.com).