Westlaw Journal
EMPLOYMENT
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 29, ISSUE 15 / FEBRUARY 18, 2015

EXPERT ANALYSIS

Employee Data Privacy Issues: Risk And Responsibility in Cyberincidents

By Valerie B. Barnhart, Esq., and Emily A. Thomas, Esq.
Kelley Kronenberg PA

Data breaches, both small and large, are occurring at an alarming pace, with companies in the United States seeing a 50 percent climb in the number of data breach investigations in 2013, when compared with 2012, according to a report last year from Trustwave Holdings Inc. Although news accounts often highlight consumer information — particularly pay-ment card data — being stolen, 45 percent of data compromises in 2013 involved non-payment card data. These statistics are particularly significant to employers because recent data breaches of employee personal information have resulted in a wrath of employee lawsuits.[1]

The odds of experiencing a data breach means that employers must be diligent in safeguarding the "personally identifiable information" of employees. Although it varies by jurisdiction, PII is generally defined as any information that, directly or indirectly, allows the identification of a particular individual. PII includes items such as an individual's Social Security number, driver's license or identification number, and financial account or credit card number, among other information.[2]

Throughout the course of the employment relationship, employers may collect, process and store various forms of PII of employees, such as bank account information for direct deposit or government-issued identification information. As a result, employers must be counseled about their cyber risk, obligations in the event of a data breach and the potential costs and consequences of a data compromise.

CYBER INSECURITY: THE NEED FOR RISK MANAGEMENT

The likelihood, and eventual long-lasting impact, of a data breach means that data risk management is at the top of employers' agendas. In fact, studies show that in the overall risk management agenda, workplace and employee privacy as well as avoiding data breaches is a chief human resources concern.[3] The days of antivirus software and firewalls making up a technical defense system are long over.

An employer must implement more stringent policies and mechanisms to minimize the risk of a data breach. Failure to comply with industry standards concerning the protection of sensitive employee data can increase the already prominent risk of a data breach, as well as hurt the employer's defense in the event of litigation. A non-exhaustive list of some risk management strategies include:

- Limiting the collection of employee PII to the least amount necessary for the accomplishment of the employers' objectives. Employee PII should be retained for only so long as is necessary and disposed of securely when the need for the PII has expired.
- Implementing requirements for password complexity. The recent report from Trustwave reveals that weak passwords permitted the initial breach intrusion in an astounding 31 percent of all breaches investigated by the company in 2013. This figure includes passwords from VPN, SSH, remote desktop and the like. Such an internal policy is wise as a technical defense strategy, but also because certain states statutorily require such reasonable security safeguards.[4]

Personally identifiable information includes items such as an individual's Social Security number, driver's license or identification number, and financial account or credit card number.

- Developing a comprehensive incident response plan. An appropriate incident response plan defines what represents a data incident, outlines the core individuals to be notified and identifies the scope of their responsibility, and provides a road map of the courses of action for an employer organization in the event of a breach. The plan should be periodically rehearsed and updated when necessary. Having a comprehensive incident response plan in place can limit the duration of a compromise and the hemorrhaging of employee PII and other data.
- Implementing strong security policies and protocols for data use, manage-ment, and disposal, including safe-guards such as staff awareness and training programs, minimizing the use and collection of personally identifiable information, and conducting privacy impact assessments.[5]
- Amending all vendor contracts, as necessary, to require compliance with the applicable, data security regulations, especially if any vendors are used by the employer to process, store, transmit or destroy employee data. Employers would be wise to similarly include a well-drafted indemnification provision for any data breach attributable to the third-party vendor to reduce liability, particularly in the event of costly litigation.
- Carrying adequate cyber liability insurance.[6] Appropriate coverage can reduce risk by covering defense and liability expenses, among other things, resulting from a data breach.[7] However, employers should not presume that current policies, such as a commercial general liability policy, would provide coverage in the event of a data breach. Like any other form of insurance, coverage can vary widely and it is crucial to understand applicable exclusions. Employers and counsel should evaluate whether coverage applies for items such as network restoration, forensic investigations, legal counsel, and externally and internally caused breaches.

BREACH COMPLIANCE REQUIREMENTS: APPLICABLE LAWS

The legal aspect of the cyberthreat landscape is constantly evolving. If, even despite adequate security measures, an employer suffers a breach, it cannot presume that only federal law, or the law of the state where the employer is located, controls its obligations. Larger or franchise organizations, and those with remote workers, often have employees in numerous geographic locations.

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands all have legislation mandating what notification steps must be taken in the occurrence of a breach of PII.[8] The statutes can vary in what constitutes a qualified data incident as well as specifies what needs to be included in the breach notification.

It is imperative for the employer organiza-tion to be aware that the law of the state in which the affected employee resides dictates any data-breach notification requirements. An organization that fails to comply with applicable notification laws runs the risk of the assessment of regulatory fines, increasing already significant potential financial exposure.

DATA DAMAGES: THE HIGH COST OF A BREACH INCIDENT

The financial losses resulting from a data breach can be devastating. Overall, an employer's financial exposure can fluctuate based on the source of the breach and the safeguards employed by the organization. On average, 2014 saw steady increases in both an organization's cost per breached record and cost per data breach incident. According to the Ponemon Institute's 2014 study on the cost of a data breach, which annually analyzes the costs incurred by U.S. companies related to data breach incidents, the average cost per compromised records climbed from $188 to $201. Overall, the total cost to an organization for a single data breach incident rose from $5.4 million to $5.9 million.

These costs can also vary depending on the attack vector. Continuing with a consistent trend, the Ponemon 2014 study reported that breaches occurring as a result of outsider threats — including hackers and malicious attacks — produced the largest cost, with the cost per breached record reaching an average of $246.

Conversely, breaches resulting from non-malicious system glitches or staff errors resulted in reduced cost-per-breached-record, at an average of $171 per record compromised from a system

glitch and $160 per record as a result of employee error caused breaches. The organization's data safeguards can also reduce the cost per compromised record. If a company has implemented an incident response plan prior to a breach, this will decrease the cost per record an average of $17.

It is important to note that employers have potential liability whether they cause the breach or are a victim of a sophisticated third-party attack or even international cyberterrorism. In the growing list of lawsuits filed recently because of data breach incidents, employers are expected to have taken precautions to secure private information, such as by following generally accepted industry standards.

Often it is not the data breach, but the employer's failure to take appropriate data security precautions, that creates potential liability.

EMPLOYEE LITIGATION IN DATA BREACH INCIDENTS

With frequent advances in technology leading to a greater risk for attacks, employee litigation is on the rise. Such lawsuits are predominantly filed in federal court as class-action lawsuits, which could result in grave exposure for an employer if the employee is able to establish the necessary elements to withstand a motion to dismiss.

Employers commonly defend against such suits based on lack of standing. In diversity actions filed in federal court pursuant to 28 U.S.C. § 1332(d)(2), a plaintiff must establish Article III standing.

To satisfy the Article III standing requirement, a plaintiff must show it has suffered an "injury in fact" that is:

- Concrete and particularized.
- Actual or imminent, not conjectural or hypothetical.
- Fairly traceable to the challenged action of the defendant.
- Will likely will be redressed by a favorable decision, as opposed to mere speculation.[9]

There is a split of authority in the lower federal courts as to whether a plaintiff's claim of increased risk of harm is sufficient to satisfy the Article III standing requirement.[10] The 7th U.S. Circuit Court of Appeals held in *Pisciotta v. Old National Bancorp* that a plaintiff has Article III standing and that the future risk of harm is sufficient to invoke jurisdiction when a plaintiff alleges his or her personal information was compromised after a security breach occurred on a defendant's website.[11]

On the other hand, the 3rd Circuit has rejected an argument that allegations of increased risk of identity theft caused by a security breach were sufficient to establish Article III standing when the harm alleged is not "sufficiently concrete and imminent."[12]

Nonetheless, recent case law demonstrates that some district courts are apt to find Article III standing if the plaintiff suffers an actual injury and not just a fear that his or her credit or identity may be compromised in the near future.[13]

Moreover, if a plaintiff is able to overcome the threshold of establishing Article III standing, he or she then must sufficiently allege a cause of action that will withstand a dismissal motion for failure to state a claim. Many of the data breach cases involve negligence, invasion-of-privacy and breach-of-contract claims. To prevail on these types of claims, a plaintiff must show he or she suffered a compensable injury that was proximately caused by the defendant's actions.

For example, in *Pisciotta,* although the 7th Circuit found the plaintiffs had Article III standing, the class-action suit was ultimately dismissed for failure to state a claim. The court found that the damages alleged, the cost of purchasing credit monitoring, was not a compensable injury.

In a case against AvMed Inc., a health care services provider in Florida, the 11th Circuit found that plaintiffs, victims of identity theft, sufficiently alleged a compensable injury. The 11th Circuit further found that the defendant's actions proximately caused the plaintiffs' alleged injury because the plaintiffs had never experienced identity theft prior to the breach, they went to considerable measures to protect their personal information and the sensitive information stolen was the same type of information used in the identity theft.[14]

Companies are encouraged to have internal policies that eliminate weak user passwords by implementing requirements for password complexity.

The law of the state in which the affected employee resides dictates any notification requirements that must be complied with as a result of a breach.

Although there are significant obstacles for an employee to prevail in an action resulting from a data breach, employers should be weary of the potential for exposure. Even where an action may not survive a motion to dismiss, there are still significant penalties that may apply if the organization has not taken the proper precautions or provided adequate notification.

This risk for exposure is not only demon-strated by the increasing number of lawsuits filed as a consequence of a data breaches, but settlement outcomes of many of these actions. For instance, recent data breaches affecting an employee-discount program provider and Sony's PlayStation Network, and the case against AvMed mentioned above, have resulted in legal settlements between $430,000 and $15 million.[15]

The recent data breaches that devastated Sony Pictures and the U.S. Postal Service serve as significant warnings of employer risk. According to a class-action complaint filed against Sony, about 47,000 Social Security numbers were compromised.[16] The data breach that occurred with the Postal Service was also catastrophic, with a potential compromise of 800,000 employees' PII nationwide.[17]

In light of rapidly advancing technology, it is essential that employers take all necessary precautions not only to protect their employees' PII, but to avoid litigation expenses and regulatory sanctions.

NOTES

[1] Trustwave Holdings Inc., 2014 Trustwave Global Security Report, *available at* http://bit.ly/1zS0KMg.

[2] *See, e.g.,* Fla. Stat. § 501.171(1)(g)(1)(a)(2014); Erika McCallister, Tim Grance and Karen Scarfone, Nat'l Inst. of Standards & Tech., Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (2010), *available at* http://1.usa.gov/1CvyhfO; Idaho Code § 28-51-104(5)(2014).

[3] Chad Brooks, *Objection! Employee Lawsuits on the Rise,* Bus. News Daily, July 10, 2014, http://bit.ly/1DFTBfH.

[4] *See, e.g.,* Fla. Stat. § 501.171(2) (2014); Mass. Gen. Laws 93H § 2 (2014).

[5] *See* Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity (2014), *available at* http://1.usa.gov/1zS2lBP. The NIST is the agency charged with developing a voluntary framework to reduce cyberrisks to critical infrastructure. The framework gathers existing global standards and best practices to help entities comprehend and manage cyberrisk.

[6] The Allianz Risk Barometer, which surveys hundreds of insurance experts globally, found that cyberrisk soared into the top 10 business risks of 2014. Allianz Risk Pulse, Allianz Risk Barometer on Business Risks 2014 (Jan. 2014), *available at* http://bit.ly/1zfVvUr.

[7] Robert P. Hartwig& Claire Wilkinson, Ins. Info. Inst., Cyber Risks: The Growing Threat (June 2014), *available at* http://bit.ly/1vsRsoy.

[8] Nat'l Conference of State Legislatures, Security Breach Notification Laws, *available at* http://bit.ly/1EGwuFg (2014).

[9] *Friends of the Earth Inc. v. Laidlaw Envtl. Servs. (TOC) Inc.,* 528 U.S. 167, 180–81 (2000).

[10] *Allison v. Aetna Inc.,* No. CIV.A. 09-2560, 2010 WL 3719243, at * 4, n. 4 (E.D. Pa. Mar. 9, 2010). The note mentions the following cases, including the brief descriptions quoted here: *Amburgy v. Express Scripts Inc.,* 671 F. Supp. 2d 1046 (E.D. Mo. 2009) ("plaintiff, who alleged that unauthorized individuals accessed a data-base containing his personal information and threatened to publicize the personal information if the defendant did not pay them a certain amount of money, lacked standing under Article III"); *McLoughlin v. People's United Bank Inc.,* No. CIVA 308CV–00944, 2009 WL 2843269 (D. Conn. Aug. 31, 2009) ("plaintiff, who claimed that unencrypted back-up tapes containing her personal information were lost or stolen but did not allege misuse, had standing"); *Ruiz v. Gap Inc. et al.,* 622 F. Supp. 2d 908 (N.D. Cal. 2009) *aff'd,* 380 F. App'x 689 (9th Cir. 2010) ("plaintiff, who alleged that laptops containing his personal information were stolen but did not allege misuse, had standing"); *Hinton v. Heartland Payment Sys.,* No. CIV. A. 09–594, 2009 WL 703139 (D.N.J. Mar. 16, 2009) ("plaintiff, who claimed that his credit information was com-promised in a electronic data breach but alleging no misuse, failed to allege an actual or imminent injury-in-fact"); *Caudle v. Towers, Perrin, Forster & Crosby Inc.,* 580 F. Supp. 2d 273 (S.D.N.Y. 2008) ("plaintiff, who alleged that laptop containing his personal information was stolen but did not allege misuse, had standing"); *Am. Fed'n of Gov't Employees v. Hawley,* 543 F. Supp. 2d 44 (D.D.C. 2008) ("plaintiff, who alleged that hard drive containing personal information was lost but did not allege misuse, had standing, although the holding was in part based on the Privacy Act of 1974").

[11] *Pisciotta v. Old Nat'l Bancorp,* 499 F.3d 629 (7th Cir. 2007).

[12] *Reilly et al. v. Ceridian Corp.,* 664 F.3d 38, 46 (3d Cir. 2011).

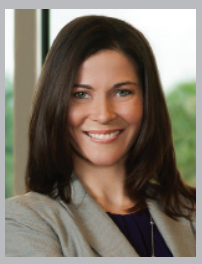
[13] *In re Adobe Sys. Privacy Litig.,* No. 13-CV-05226, 2014 WL 4379916, at * 8 (N.D. Cal. Sept. 4, 2014) (holding the plaintiffs sufficiently alleged Article III standing where "the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates ... [and] plaintiffs' personal information was among the information taken during the breach."); *Resnick v. AvMed Inc.,* 693 F.3d 1317 (11th Cir. 2012) (holding the allegations that plaintiffs were the victims of identity theft and suffered monetary loss following the data breach were sufficient to establish Article III standing); *Burrows v. Purchasing Power LLC,* No. 1:12-CV-22800, 2012 WL 9391827 (S.D. Fla. Oct. 18, 2012) (finding Article III standing where the plaintiff alleged he suffered a monetary loss when he was not able to get his tax refund because another individual falsely filed a tax return using the plaintiff's identity); *see also In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* 996 F. Supp. 2d 942 (S.D. Cal. 2014) (finding standing based on "plausibly alleged ... 'credible threat' of impending harm"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.,* No. MDL 2360, 2014 WL 1858458 (D.D.C May 9, 2014) (finding risk of identity theft alone was not sufficient to confer standing but finding that one plaintiff's allegations that he received a letter in the mail thanking him for applying for a loan and another plaintiff's allegations that she received phone calls from insurance companies regarding her medical conditions were sufficient to confer Article III standing). This issue is on appeal again in the 7th Circuit after a Chicago federal judge dismissed a putative class-action suit against Neiman Marcus over a 2013 data breach at the high-end retailer. *Remijas et al. v. Neiman Marcus Group,* No. 14 C 1735, 2014 WL 4627893 (N.D. Ill., E. Div. Sept. 16, 2014). The judge found the plaintiffs' alleged increased risk of identity theft and financial fraud were insufficient injuries for purposes of Article III. The plaintiffs appealed, saying they suffered an injury when Neiman Marcus allowed the theft to occur, regardless of whether hackers make fraudulent charges on the customers' cards or sell their stolen information. *Remijas et al. v. Neiman Marcus Group,* No. 14-3122, *appellants' reply brief filed* 2014 WL 7278604 (7th Cir. Dec. 19, 2014). The case was argued before the appellate panel Jan. 23.

[14] *Resnick*, 693 F.3d 1317.

[15] *Resnick et al. v. AvMed Inc.,* No. 1:10-cv-24513, *order approving final settlement* (S.D. Fla. Feb. 28, 2014), resulted in a settlement of $3 million. *Burrows v. Purchasing Power LLC,* No. 12-cv-22800, *final judgment issued* (S.D. Fla. Oct. 7, 2013) resulted in a settlement of approximately $430,000. Additionally, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* MDL-No.-2258, *preliminary approval of settlement order* (S.D. Cal. July 10, 2014) resulted in a settle-ment of $15 million, which has been preliminarily approved by U.S. District Judge Anthony J. Battaglia of the Southern District of California, who is overseeing the case.

[16] *Corona et al. v. Sony Pictures Entm't,* No. 2:14-cv-09600, *complaint filed* 2014 WL 7113706 (C.D. Cal. Dec. 14, 2014).

[17] Doina Chiacu, *U.S. Postal Service Data Breach May Compromise Staff, Customer Details,* Reuters, Nov. 10, 2014, http://reut.rs/1CZIAr4.



Valerie Barnhart (L) is a partner with the national, full-service law firm **Kelley Kronenberg PA**. She represents businesses in data privacy and security matters, business transactions, and business litigation. She can be reached at vbarnhart@kelleykronenberg.com. **Emily Thomas** (R) is an attorney with Kelley Kronenberg. She focuses her practice on business transactions and all aspects of business and commercial litigation from trial to the appellate level. She can be reached at ethomas@kelleykronenberg.com.