Bloomberg BNA

Privacy and Security Law Report®

Recent Trends in Data Security Class Actions And Considerations for Minimizing the Risk of Such Cases



BY KRISTOFOR T. HENNING, THOMAS J. SULLIVAN, AND FRANCO A. CORRADO

Corporate general counsel and public company directors rank data security issues among their top concerns.[1] Indeed, news of high-profile data security breaches has grabbed headlines in 2012 and many such cases have made their way through the courts of late. Lawmakers have taken notice as well—legislation aiming to create a national standard for data breach disclosures is meandering its way through the Senate and the calls for Congress to update what many believe to be an antiquated Privacy Act of 1974 have grown louder.[2] The Federal Trade Commission also has been actively prosecuting enforcement actions over data collection and storage practices and the transparency of privacy policies, and issued a report dictating best practices for businesses that possess personal data.[3] The plaintiffs' bar is closely and carefully monitoring these developments and modifying its tactics in response to judicial developments.

Data breaches have become a fact of life for many businesses in this age of electronic commerce.[4] Since

[1] Corporate Board Member and FTI Consulting, *Legal Risks on the Radar* 2–3 (Aug. 13, 2012), *available at* http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf.

Kristofor T. Henning, a litigation partner and member of the Class Action Steering Committee and Working Group at Morgan, Lewis & Bockius LLP, in Philadelphia, handles a broad variety of commercial litigation with an emphasis on class action defense. The practice of Thomas J. Sullivan, also a litigation partner and member of the Class Action Steering Committee and Working Group at the firm's Philadelphia office, encompasses a variety of commercial and product liability litigation focusing on class action defense, mass torts, and other complex commercial litigation. Franco A. Corrado, an associate in the firm's Philadelphia office, focuses on a broad range of commercial and civil litigation with an emphasis on consumer class actions and complex commercial disputes.

[2] *See, e.g.*, U.S. Gov't Accountability Office, GAO-12-961T, *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape* (released July 31, 2012), *available at* http://www.gao.gov/assets/600/593150.txt; *see also* Allison Grande, *Government Must Tweak Privacy Protections For New Era, Panel Hears*, Law360 (July 31, 2012, 9:40 PM), http://www.law360.com/articles/364181.

[3] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC Report] (11 PVLR 590, 4/2/12).

[4] *E.g.*, Sasha Romanosky, David A. Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation* 1 (Temple University Legal Studies Research Paper No. 2012-30, Feb. 19, 2012) (unpublished article), *available at* http://ssrn.com/abstract=1986461.

 ISSN 1538-3423

2005, there have been an estimated 2,800 data breaches resulting in 543 million lost or compromised records.[5] According to a 2011 survey, approximately 90 percent of companies reported experiencing at least one data breach.[6] The monetary impact of data breaches can be significant, with the cost in 2011 averaging roughly $5.5 million (or about $194 per compromised record) for breaches involving fewer than 100,000 records.[7] Litigation expenses can be a major component of these costs.[8] Although only about 4 percent of reported data breaches result in federal litigation, a number of factors can significantly increase litigation risk such as the number of records compromised in the breach, the type of information contained in the affected records[9] and the underlying cause of the breach.[10]

This article provides a basic overview of the data security class action landscape and current trends. It examines theories advanced by plaintiffs and delves into the courts' responses to these theories, and offers suggestions for minimizing the risks of such actions.

PLAINTIFFS' CAUSES OF ACTION AND THEORIES OF HARM

Plaintiffs have advanced a number of different theories in data breach litigation. In the first quantitative study of federal data breach litigation, researchers identified over 86 unique causes of action, including 34 tort claims, 15 contract claims, and a plethora of claims based on state and federal statutes.[11] Claims have surfaced in a multitude of forms, ranging from those for the violation of various federal and state breach notification laws to claims for violation of state consumer protection statutes, and even to claims for trespass to chattels. The range of damages theories is equally broad, with plaintiffs seeking compensation not only for alleged financial losses stemming from identity theft, but also credit monitoring costs, emotional distress damages and statutory penalties. Such claims have been met with mixed results.

Generally speaking, plaintiffs have avoided the dismissal of claims when they have been able to plead specific facts regarding economic harm from the alleged misuse or unlawful collection of their data. Plaintiffs have also experienced moderate success alleging violations of state data breach and consumer protection statutes. Although a comprehensive analysis of the 46 different state notification laws is beyond the scope of this article, critical differences exist among these statutes—such as the definition of a triggering event[12]—that may create fertile ground for litigation based on technical noncompliance. Considerable variations also exist among state consumer protection statutes, with some potentially friendlier than others due to their broad definitions of injury and relaxed standing requirements.[13]

JUDICIAL RESPONSE TO PLAINTIFFS' CLAIMS AND THEORIES

Data breach claims can generally be divided into two categories based on the nature of the alleged injury: (1) those where plaintiffs allege a present injury (e.g., actual financial loss from identity theft) and (2) those where plaintiffs allege some type of prospective harm (e.g., an increased risk of identity theft). Plaintiffs alleging actual loss are more likely to avoid dismissal than those alleging some type of prospective harm.[14] As discussed below, two main cases stand out as exceptions to this general observation and plaintiffs have apparently noticed this trend.[15]

In efforts to survive the pleading stage, plaintiffs have recently employed several novel strategies to overcome

[5] *Id.*

[6] *See, e.g.*, Ponemon Inst., *Perceptions About Network Security: Survey of IT & IT Security Practitioners in the U.S.* 3 (June 2011), *available at* http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.

[7] *Id.*

[8] *See* Ponemon Inst., *2010 Annual Study: U.S. Cost of a Data Breach* 4 (March 2010), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach (describing the various expenses that contribute to the total cost of an average data breach, including litigation costs) (10 PVLR 418, 3/14/11).

[9] *See* Romanosky et al., *supra* note 4, at 3 (reporting that a data breach is six times more likely to result in federal litigation if it involves financial information).

[10] *Id.* (reporting that a data breach is three times more likely to result in federal litigation if it is caused by the improper disposal of information rather than loss or theft).

[11] *Id.* at 22.

[12] *Compare* N.J. Stat. Ann. § 56:8-161(10) (West 2006) (''[U]nauthorized *access* to [unencrypted] electronic . . . data containing personal information . . . .'' (emphasis added)), *with* Cal. Civ. Code § 1798.29(a) (West 2003) (''[U]nencrypted personal information . . . is *reasonably believed* to have been . . . acquired . . . .'' (emphasis added)), *and* Fla. Stat. Ann. § 817.5681(10) (West 2005) (''[N]otification is not required if . . . the person *reasonably determines that the breach . . . will not likely result in harm* to the [affected] individuals . . . .'' (emphasis added)).

[13] *See, e.g.*, N.Y. Gen. Bus. Law § 349 (McKinney 2012) (providing a cause of action for a deceptive, consumer-oriented business practice when the deceptive practice results in an ''actual,'' but not necessarily pecuniary, injury); *see also Bose v. Interclick, Inc.*, No. 10-CV-09183, 2011 WL 4343517, at *1, *9 (S.D.N.Y. Aug. 17, 2011) (holding that absence of pecuniary harm arising from defendant's conduct did not preclude a deceptive trade practices claim under Section 349) (10 PVLR 1235, 9/5/11); Romanosky et al., *supra* note 4, at 22 (stating that of the 231 cases examined, approximately 180 involved a cause of action under a state unfair business practices statute).

[14] *Compare Resnick v. AvMed, Inc.*, No. 11-13694, 2012 WL 3833035, at *4–5 (11th Cir. Sept. 5, 2012) (reversing order granting motion to dismiss where plaintiffs alleged financial loss following identity theft after two laptop computers containing unencrypted confidential information were stolen from defendant) (11 PVLR 1413, 9/17/12), *with Reilly v. Ceridian Corp.*, 664 F.3d 38, 41 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012) (10 PVLR 1859, 12/19/11), *and Whitaker v. Health Net of Cal.*, No. 2:11-cv-00910, 2012 WL 174961, at *1, *3 –4 (E.D. Cal. Jan. 20, 2012) (loss of hardware containing plaintiffs' personal information) (11 PVLR 195, 1/30/12). *See also Burrows v. Purchasing Power, LLC*, No. 12-cv-22800, slip op. at 4–6 (S.D. Fla. Oct. 18, 2012) (finding alleged lost federal tax refund allegedly resulting from data theft satisfied Article III injury-in-fact requirement) (11 PVLR 1587, 10/29/12).

[15] *See Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 631–34 (7th Cir. 2007) (plaintiffs purchased credit monitoring services following cyber-attack on banking website) (6 PVLR 1374, 9/3/07); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140–41 (9th Cir. 2010) (plaintiffs purchased credit monitoring services following theft of laptop containing unencrypted personal information) (9 PVLR 1729, 12/20/10).

  PVLR ISSN 1538-3423

a lack of actual economic injury. Such strategies have included alleging esoteric torts such as trespass to chattels and arguing that personal information has an independent economic value.

■ Allegations of Future Harm Arising from a Data Breach Typically Do Not Constitute an Article III Injury-in-Fact.

Under Article III, Section 2 of the U.S. Constitution, the power of the federal courts is limited to the resolution of actual ''cases or controversies.'' A case or controversy exists when a party has a personal stake in the outcome of a case, which the party demonstrates by establishing his/her/its standing to sue in court.[16] Under Article III, that is done by showing (1) that the plaintiff suffered an injury-in-fact, (2) a causal relationship between his/her/its injury and the defendant's conduct, and (3) the likelihood that the injury will be redressed by a favorable decision.[17]

Article III's injury-in-fact requirement, in particular, has been a focal point in data privacy litigation. A number of federal courts have refused to recognize future harm arising from a data breach as an Article III injury-in-fact and have held that plaintiffs' alleged increased risk of identity theft and the credit monitoring costs allegedly incurred to minimize this risk are too speculative to support Article III standing.[18] In *Reilly v. Ceridian Corp.*, for instance, the Third Circuit emphasized Article III's injury-in-fact requirement, explaining that the ''present test is actuality, not hypothetical speculations concerning the possibility of future injury.''[19] This test is not met where there is ''no evidence suggest[ing] that the data has been—or will ever be—misused.''[20]

Reilly effectively illustrates the challenge plaintiffs have faced in the data security class action context. In that case, the personal information of 27,000 employees at 1,900 companies allegedly was compromised when Ceridian was victimized by a cyber-attack.[21] Although Ceridian acknowledged that its firewall had been penetrated, it could not determine whether the hacker accessed, or even understood, its data.[22] Ceridian also offered one year of free credit monitoring and identity theft protection to affected individuals. A class action followed nonetheless, alleging claims for negligence and breach of contract because, according to the plaintiffs, they incurred credit monitoring costs and faced an increased risk of identity theft as a result of Ceridian's alleged failure to adequately protect their personal information.[23] Ceridian successfully moved to dismiss on the ground that the plaintiffs' complaint failed to demonstrate a cognizable injury.[24]

The Third Circuit affirmed the district court's dismissal, holding that the plaintiffs' alleged increased risk of identity theft was too conjectural to constitute an Article III injury-in-fact[25] because, among other reasons, the claim relied on mere speculation that the hacker acquired the plaintiffs' personal information and possessed both the intent and technical skill to commit identity theft.[26] The Third Circuit also refused to recognize the plaintiffs' credit monitoring costs as an Article III injury-in-fact on the ground that these costs were incurred to avoid speculative future injury.[27]

Notably, the *Reilly* plaintiffs' reliance on *Pisciotta v. Old National Bancorp*[28] and *Krottner v. Starbucks Corp.*,[29] two circuit court decisions frequently cited for the proposition that an increased risk of identity theft constitutes an Article III injury-in-fact, was unavailing. The court disagreed with *Pisciotta*'s and *Krottner*'s respective comparisons of the injury in data breach cases to the injury in environmental contamination and defective medical device cases.[30]

The rationale for finding standing in those cases ''hinges on human health concerns,'' where the ''injury'' is committed the moment the ''defective device[s]'' or ''toxic substance[s]'' are introduced to the human body even though the extent of the injury may not be quantifiable until some later time. By contrast, the court concluded that in a data breach case, there is no injury before the data is misused, and the prospective risk of injury hinges on the unpredictability of a future criminal act by a third party.[31] Further, the harm associated with injuries to the body and the environment are ''unique,'' and may not be wholly redressable through money damages; whereas, should the prospective injury materialize in a data breach case, a plaintiff could adequately be returned to his or her original position through monetary compensation.[32]

Federal district courts in California and New York have likewise dismissed claims in which the plaintiffs sought recovery for unspecified harm and/or the increased risk of future harm. In *Whitaker v. Health Net of California, Inc.*, the U.S. District Court for the Eastern District of California rejected claims that the defendant's loss of hardware containing personal information could give rise to a claim based on prospective fu-

[16] *Raines v. Byrd*, 521 U.S. 811, 818 (1997); *Baker v. Carr*, 369 U.S. 186, 204 (1962).

[17] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992).

[18] *See Reilly*, 664 F.3d at 41 (hackers infiltrated payroll-processing firm's database); *Holmes v. Countrywide Fin. Corp.*, No. 08-cv-00205, 2012 WL 2873892, at *14 (W.D. Ky. July 12, 2012) (rejecting claims under Kentucky and New Jersey consumer protection laws alleging losses in the form of credit monitoring costs) (11 PVLR 1209, 7/30/12); *Whitaker*, 2012 WL 174961, at *1, *3–4 (loss of hardware containing plaintiffs' personal information); *Hammond v. The Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307, at *1–2 (S.D.N.Y. June 25, 2010) (same); *Ponder v. Pfizer*, 522 F. Supp. 2d 793, 797–98 (M.D. La. 2007) (employees' personal information compromised after file-sharing software installed and used on laptop); *Bell v. Acxiom Corp.*, No. 4:06CV00485, 2006 WL 2850042, at *1–2 (E.D. Ark. Oct. 3, 2006) (theft and sale of clients' personal information by hackers) (5 PVLR 1431, 10/16/06).

[19] *Reilly*, 664 F.3d at 43.

[20] *Id.*

[21] *Id.* at 40.

[22] *Id.*

[23] *Id.*

[24] *Id.* at 41.

[25] *Id.* at 41–43.

[26] *Id.*

[27] *Id.* at 45–46.

[28] *Pisciotta*, 499 F.3d at 634 (holding that plaintiffs who had not suffered actual financial loss due to data breach had standing to seek recovery of credit monitoring costs).

[29] *Krottner*, 628 F.3d at 1140–41 (holding that credible threat of identity theft is sufficient to establish Article III standing).

[30] *Reilly*, 664 F.3d at 44–46 (citations omitted).

[31] *Id.* at 45.

[32] *Id.*

ture losses.[33] The same result followed in *Hammond v. The Bank of New York Mellon Corp.*, with the court noting that when a plaintiff '' 'surmises that, as a result of a security breach, he or she faces an increased risk of identity theft at an unknown point in the future' the 'claimed injury is in the realm of the hypothetical . . . [and] do[es] not provide the injury-in-fact required for Article III standing.' ''[34]

This is not to say that plaintiffs alleging prospective harm will never be able to establish an Article III injury-in-fact. Although the Third Circuit in *Reilly* criticized the analogies at the heart of *Pisciotta* and *Krottner*, it also recognized that the facts in those cases provided a stronger basis for finding Article III standing.[35] More specifically, the court reasoned that *Pisciotta* involved a ''sophisticated, intentional, and malicious'' intrusion by hackers into a company's network, and *Krottner* involved the theft of a laptop containing unencrypted personal information. In *Reilly*, however, the data in question may not actually have been accessed, and even if it had, it may not have been deciphered, and ''no identifiable taking had occurred'' in any event.[36] According to the Third Circuit, these critical facts rendered the future harm in *Pisciotta* and *Krottner* ''significantly more 'imminent' and 'certainly impending' '' than the future harm alleged by the *Reilly* plaintiffs.[37] Issues of standing will continue to be litigated intensely.

■ Courts Have Generally Held That Plaintiffs' Personal Information Does Not Have Inherent Economic Value.

In light of the weight of the foregoing authority, some plaintiffs have attempted to compensate for a lack of actual economic injury by arguing that their personal information has independent economic value. Courts have largely rejected such arguments.[38] For instance, the plaintiff's consumer protection claims under California law were dismissed in *LaCourt v. Specific Media* because the court found that the plaintiffs' personal data did not have inherent economic value, and particularized economic loss as a result of the tracking was necessary to state a claim. Additionally, in *Low v. LinkedIn Corp.*, the plaintiff complained about the defendant's alleged practice of tracking users' internet browsing history to then transfer it to third-party advertising and marketing companies. But, because the plaintiff could neither identify which sensitive personal information was (or was likely to be) published nor point to any economic harm from the alleged publication, the complaint was dismissed. Defendants have not been completely successful in such cases, however.[39]

In *Claridge v. RockYou*, the plaintiff allegedly lost ''some ascertainable but unidentified 'value' and/or property right inherent in [his personal information]'' when an online services developer's network was hacked and the plaintiff's login credentials to social networking sites were taken, allegedly as a result of RockYou's failure to implement commercially reasonable safeguards for its applications and services.[40] It is noteworthy that in a letter notifying customers of the breach, RockYou apparently acknowledged that its substandard information safeguards contributed to the breach.[41] The district court expressed ''doubts about plaintiff's ultimate ability to prove his damages theory,'' and left the door open for a future dispositive motion if discovery revealed ''no basis . . . upon which plaintiff could legally demonstrate tangible harm,'' but nevertheless held that the plaintiff had alleged injury-in-fact standing sufficient to survive a motion to dismiss.[42]

Fraley v. Facebook Inc. involved similar allegations with regard to Facebook's Sponsored Stories feature, which displayed user images alongside advertiser products or services that the user ''liked.''[43] Plaintiffs claimed that this practice was tantamount to a misappropriation of their images and personal endorsements, and brought suit under a variety of California statutes, including a right-to-publicity statute, over Facebook's failure to compensate them for these alleged endorsements. The court denied Facebook's motion to dismiss because it found that the company generated advertising revenue through the Sponsored Stories feature.[44]

---

[33] *Whitaker*, 2012 WL 174961, at *2 (branding prospective harm stemming from loss of plaintiffs' data as ''precisely the type of conjectural and hypothetical harm that is insufficient to allege standing'').

[34] *Hammond*, 2010 WL 2643307, at *6; *see also Gaos v. Google, Inc.*, No. 10-CV-4809, 2012 WL 1094646, at *2 (N.D. Cal. Mar. 29, 2012) (granting motion to dismiss nonstatutory claims because no proof of injury resulting from unauthorized dissemination of search queries, and information disclosed, did not create inference of imminent danger or harm) (11 PVLR 639, 4/9/12); *Paul v. Providence Health Sys.*, 273 P.3d 106, 114 (Or. 2012) (plaintiffs alleged that defendant failed to protect and safeguard stolen information, but claim was dismissed because information was never viewed or misused) (11 PVLR 422, 3/5/12).

[35] *Reilly*, 664 F.3d at 44 (citations omitted).

[36] *Id.* (citations omitted).

[37] *Id.* (citations omitted).

[38] *See Low v. LinkedIn Corp.*, No. 11-CV-01468, 2011 WL 5509848, at *1, *4 (N.D. Cal. Nov. 11, 2011) (dismissing claim because economic value of personal information allegedly accessed was ''too abstract and hypothetical'' to establish standing) (10 PVLR 1681, 11/21/11); *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256, 2011 WL 1661532, at *1, *45 (C.D. Cal. Apr. 28, 2011) (holding that plaintiffs lacked Article III standing, in part, because they did not allege particularized economic harm arising from unauthorized collection and disclosure of personal information); *Bose*, 2011 WL 4343517, at *7 (holding that unauthorized tracking of information, without more, is insufficient to state a claim under the Computer Fraud and Abuse Act).

[39] *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 860–61 (N.D. Cal. 2011) (denying motions to dismiss for lack of standing and failure to state a claim where plaintiff alleged loss in value of social networking log-in credentials due to data breach) (10 PVLR 620, 4/25/11); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 797–99, 811–12 (N.D. Cal. 2011) (denying motion to dismiss where social networking site allegedly failed to compensate plaintiffs for unauthorized use of their likenesses) (11 PVLR 25, 1/2/12).

[40] *Claridge*, 785 F. Supp. 2d at 865.

[41] *Id.*

[42] *Id.*

[43] *Fraley*, 830 F. Supp. 2d at 791–92.

[44] *Id.* By way of further background, the parties have since attempted to settle this matter. A first proposed settlement was rejected by the district court because, among other reasons, there was no cash component to the class compensation (11 PVLR 1343, 9/3/12). *See* Nate Raymond, *Facebook Pitches New $20 million ''Sponsored Stories'' Settlement*, Reuters (Oct. 8, 2012), *available at* http://www.reuters.com/article/2012/10/08/us-facebook-settlement-idUSBRE89712220121008. A modified proposal was submitted for the court's approval Oct. 5, which included cash compensation to the class (11 PVLR 1526, 10/15/12). *Id.*

  PVLR ISSN 1538-3423

■ **At Least One Court Has Denied a Motion to Dismiss a Claim for Trespass to Chattels.**

At least one plaintiff avoided dismissal with a theory that the defendant's alleged unauthorized tracking of online activity amounted to a trespass to chattels.[45] In *Bose v. Interclick, Inc.*, the defendant's alleged use of ''flash cookies,'' which track computer users' online activities without their consent, was the subject of the claim.[46] As alleged, the flash cookies interfered with the computer's performance, thus giving rise to the trespass to chattels claim.[47] Although the district court was clearly skeptical of the plaintiff's ultimate prospects, it held that the adverse impact allegedly caused by the defendant's flash cookies was ''arguably sufficient'' to state a claim for trespass to chattels and denied the defendant's motion to dismiss.[48]

Based on these and other similar rulings, one can expect plaintiffs to try more theories as the case law continues to evolve.

CONSIDERATIONS FOR MINIMIZING EXPOSURE TO DATA BREACH LITIGATION

An ounce of prevention continues to be worth a pound of cure, and if a business engages in the collection and storage of personally identifiable information, it should consider implementing appropriate safeguards to protect against data security breaches. Although there is no one-size-fits-all approach, state and federal statutes are one source of guidance for security best practices.[49] Along those lines, companies should consider developing written policies governing the collection, use, storage, transmission, and destruction of personal information compliant with applicable laws, as well as training relevant employees on these policies.

Vendor and business partner agreements are often overlooked, which can be prove to be a costly mistake. A recent study found that nearly 76 percent of data breach investigations were triggered by security deficiencies introduced by third parties.[50] A business which outsources data system support, development, or maintenance to vendors or business partners that are granted access to personal information should think about incorporating information security protocols and policies into those agreements.[51] Reporting and oversight requirements in those agreements could be another helpful means of ensuring vendor compliance.[52]

As a further risk minimization measure, companies might consider crafting a planned response to data security compromises. The FTC's ''best practices'' can serve as a starting point, but response plans should be tailored to the individual business.[53] Data security experts and forensic computer specialists versed in identifying sources of breaches and restoring a system's integrity could prove helpful in guarding against data security compromises. Enlisting the services of experienced outside counsel could help preserve legal privileges that would shield the work from discovery, which could potentially mean the difference between generating a useful investigative report and producing a ''road map'' for prospective litigants.[54] Counsel could also help navigate applicable disclosure and notification laws should a breach occur.

If a security breach were to occur, steps can be taken to help manage the risk of litigation and/or the attendant exposure. Developing and implementing clear, conspicuous warnings and disclosures in privacy policies and customer agreements could lay the foundation for effective affirmative defenses and other types of defenses. Also consider incorporating class action waiver provisions and provisions capping consequential damages to potentially blunt the significant financial threat often associated with class action litigation.[55] These disclosures/agreements may be more effective when users are required to acknowledge that they have read and understand the terms of the service/user agreement and privacy policy.[56]

---

[45] Trespass to chattels is a tort where one party physically interferes with another's possession of personal property. *Restatement (Second) of Torts* § 218 cmt. e (1964).

[46] *Bose*, 2011 WL 4343517, at *7.

[47] *Id.* at *9–11.

[48] *Id.*

[49] *See, e.g.*, 201 Mass. Code Regs. 17.04(3)–(6) (2012) (requiring any entity that stores or transmits personal information to, among other things, encrypt data that will be stored on portable devices or transmitted wirelessly and provide up-to-date firewall protection for data stored on systems connected to the internet).

[50] Trust Wave, *2012 Global Security Report, Executive Summary* 1 (Feb. 7, 2012), *available at* https://www.trustwave.com/lp/global-security-b?utm_expid=50006280&utm_referrer=http%3A%2F%2Fwww.sourcingspeak.com%2F2012%2F05%2Fdata-security-protections-inoutsourcing-agreements.html.

[51] Jeffrey D. Hutchins, *Outlining Data Protection In Outsourcing Agreements*, Law360 (June 7, 2012, 3:56 PM), http://www.law360.com/privacy/articles/348088/outlining-data-protection-in-outsourcing-agreements.

[52] *Id.*

[53] *See* FTC Report, *supra* note 3.

[54] Lisa J. Sotto, John W. Woods Jr. & John J. Delionado, *Data Breach! Correct Response Crucial*, N.Y. L.J. (May 29, 2007), *available at* http://www.hunton.com/files/Publication/24c006a8-60cd-473c-9320-b2c22c80bd28/Presentation/PublicationAttachment/e3382668-161e-44b7-af2b-ae5138334d24/NYLJ_DataBreach.pdf.

[55] The United States District Court for the Southern District of New York recently enforced an arbitration clause and granted the defendants' motion to compel arbitration on an individual basis in a putative class action alleging violations of state consumer protection and identity theft statutes and several common law claims over a security breach allegedly resulting in identity theft. *See, e.g.*, *Orman v. Citigroup, Inc.*, 1:11-cv-07086, 2012 WL 4039850, at *3–4 (S.D.N.Y. Sept. 12, 2012) (11 PVLR 1412, 9/17/12). Notably, the court rejected the plaintiffs' argument that compelling individual arbitration would result in the ''prospective waiver'' of protected statutory rights because the ''vindication of statutory rights analysis'' under the Federal Arbitration Act plaintiffs sought to invoke did not apply to their attempted state law claims. *Id.* Likewise, in *Sherf v. Rusnak/Westlake*, No. B237275, 2012 WL 4882547, at *1 (Cal. App. 2d Oct. 16, 2012), a California appellate court held that the U.S. Supreme Court's decision in *AT&T Mobility LLC v. Concepcion* invalidated California state law barring class action waiver provisions, but remanded for a determination of whether the particular arbitration provision at issue was unconscionable under general principles of California law. *Id.* (discussing *Concepcion*, 131 S. Ct. 1740 (2011)).

[56] Several federal district courts have granted defendants' motions to compel arbitration where the arbitration agreements consisted of clauses in electronic agreements that customers were prompted, but not required, to review. *See Vernon v. Qwest Commc'ns Int'l, Inc.*, No. 09-01840, 2012 WL 768125, at *1, *11–14, *22 (D. Colo. Mar. 8, 2012) (granting defendant internet service providers' motion to compel arbitra-

Defenses to litigation could also be enhanced through proactive measures, such as alerting credit reporting agencies and/or providing identity theft insurance to persons whose information was or may have been accessed. These offerings can preserve customers' goodwill, with the potential added benefit of laying the foundation for a defense to class certification.[57]

In closing, further developments in this area of the law by the courts, regulatory agencies, and state and federal governments are a certainty. Plaintiffs' lawyers will be monitoring these trends, and will continue to adjust their pleading strategies accordingly. Effective risk mitigation strategies and aggressive pleading challenges will likely serve as the optimum antidotes to safeguarding against the risk of a data security class action.

---

tion where putative class members clicked ''I accept'' after being directed to review customer agreement containing arbitration clause that was accessible via hyperlink); *Swift v. Zynga Game Network, Inc.*, 805 F. Supp. 2d 904, 911–12 (N.D. Cal. 2011) (granting motion to compel arbitration where putative class members were directed to review customer agreement containing arbitration clause by clicking on hyperlink prior to using defendant's services).

[57] There are a number of examples where courts denied class certification in consumer class actions because voluntary recall and/or refund programs implemented by defendants represented superior methods of compensating putative class members. *E.g.*, *Webb v. Carter's Inc.*, 272 F.R.D. 489 (C.D. Cal. 2011) (denying certification, among other reasons, because of refund and reimbursement policy); *In re Aqua Dots Prods. Liab. Litig.*, 270 F.R.D. 377 (N.D. Ill. 2010) (''Where available refunds afford class members a comparable or even better remedy than they could hope to achieve in court, a class action would merely divert a substantial percentage of the refunds' aggregate value to the class lawyers.'').

  PVLR ISSN 1538-3423