



Fox Rothschild LLP
ATTORNEYS AT LAW

Litigation Roundup

**Practising Law Institute
Cybersecurity 2014:
Managing the Risk**

September 10, 2014

Presented by:
Scott L. Vernick, Esq.



Litigation Landscape

- The scope and number of cases arising from data breaches continue to increase.
 - In the first quarter of 2014, plaintiffs filed 178 class action complaints related to data security breaches.
 - 77% of these cases involved data *privacy* (i.e., the collection, use, and sharing of personal information);
 - 23% of these cases involved data *security* (safeguarding information, and data security breaches).

Source: *Shifting Trends: Privacy & Security Class Action Litigation*,
Bryan Cave, June 2014

Litigation Landscape

- Over 70 complaints filed against Target alone.
- More recently, customers have also launched class actions related to data security breaches against:
 - P.F. Chang's (June 2014);
 - Supervalu (July 2014);
 - eBay (July 2014); and
 - Community Health Systems (August 2014).

Litigation Landscape

- Litigation related to data security breaches adds to the already high costs associated with a breach.
 - In 2013, data breaches cost organizations an average of \$5.4 million.
 - \$201 per record (up from \$188 per record in 2012).

Source: 2014 Cost of Data Breach Study, Ponemon Institute.

Litigation Landscape

- Costs include:
 - Direct costs (investigations, notifications, legal fees and expenses); and
 - Litigation has resulted in settlements in the millions (e.g., \$3 million by AvMed, Inc., \$15 million by Sony, \$1.25 million by LinkedIn Corp., and a proposed \$8.5 million settlement by Google).

Litigation Landscape

- Costs include:
 - Indirect costs (lost business, public relations, expenses to preserve and restore reputation).
- Compare to costs of having preventative measures in place (e.g., policies related to passwords, encryption, firewalls, mobile devices), and training employees.

Litigation Landscape

- Examples of potential plaintiffs:
 - Customers and/or employees.
 - Financial institutions (Banks and Credit Unions).
 - Shareholders.

Theories of Liability

Customers and/or Employees

- Customers and/or employees typically allege the following causes:
 - Negligence, breach of contract, breach of implied covenant, breach of fiduciary duty, and invasion of privacy.
 - Violations of state notification statutes, unfair competition, and consumer protection laws (e.g., deceptive/unfair trade practices acts).
 - Violations of Computer Fraud and Abuse Act, Electronic Communications Privacy Act, or Stored Communications Act.

Theories of Liability Financial Institutions

- Similar legal theories as consumer class actions, but seek damages for lost business, reimbursement for fraud, and other breach-related expenses, such as the reissuance of payment cards, and the administrative cost of customer notification.

Theories of Liability Financial Institutions

- For example, Umpqua Bank brought a class action on behalf of financial institutions against Target in which it seeks actual damages, compensatory damages, and punitive damages. *See Umpqua Bank v. Target Corp.*, No. 14-cv-00643 (D. Minn.).
- Umpqua Bank alleges that financial institutions incurred damages from reissuing payment cards, refunding charges, and notifying customers.

Theories of Liability Shareholders

- Shareholders typically allege the following causes of action: breach of fiduciary duty, abuse of control, gross mismanagement, and waste of resources against corporate officers and directors.
 - Shareholders argue that board members and executives knew, or should have known, that the company failed to meet industry standards, leaving consumer information vulnerable to cyberattack.
 - Four separate derivative class actions have been brought against Target by its shareholders.
 - See e.g., *Collier v. Steinhafel*, No. 14-cv-00266 (D. Minn.).

Trends in How Courts Have Ruled

- Historically, courts dismissed data breach cases because plaintiffs failed to allege Article III standing.
 - A “credible threat of harm” that is “both real and immediate, not conjectural or hypothetical.”
 - *e.g.*, increased risk of identity theft.

Trends in How Courts Have Ruled

- Even in the few instances where courts decided that plaintiffs had standing, courts dismissed the cases for failure to allege damages.
 - A “cognizable injury” (i.e., economic injury or actual pecuniary loss).
 - *e.g.*, financial fraud, unreimbursed charges.

Plaintiffs Lack Standing

- *In re LinkedIn User Privacy Litig.* (N.D. Cal.):
 - Plaintiffs filed complaint against LinkedIn over a data breach incident in which approximately 6.5 million users' passwords and email addresses were stolen and posted on the Internet.
 - Plaintiff argued that they had standing to sue because they suffered economic harm by not receiving the full benefit of the bargain they paid for premium memberships.
 - On March 6, 2013, the Court granted LinkedIn's motion to dismiss the complaint.

Plaintiffs Lack Standing

- *In re LinkedIn User Privacy Litig.* (N.D. Cal.):
 - The Court held that, “[t]o satisfy Article III standing, plaintiff must allege:
 - An injury-in-fact that is concrete and particularized, as well as actual and imminent;
 - That injury is fairly traceable to the challenged action of the defendant; and
 - That it is likely (not merely speculative) that injury will be redressed by a favorable decision.”

Plaintiffs Lack Standing

- *In re LinkedIn User Privacy Litig.* (N.D. Cal.):
 - Plaintiffs failed to allege that “included in Plaintiffs’ bargain for premium membership was the promise of a particular (or greater) level of scrutiny that was not part of the free membership.”
 - Plaintiffs did not allege that they relied upon (or even read) LinkedIn’s representations regarding safeguarding personal information.
 - Plaintiffs’ allegation that their LinkedIn passwords were “publicly posted on the Internet” does not amount to a “legally cognizable injury, such as, for example, identity theft or theft of personally identifiable information.”

Plaintiffs Lack Standing

- *In re Barnes & Noble Pin Pad Litigation* (N.D. Ill.):
 - Skimmers placed on PIN pad devices at 63 locations.
 - Plaintiffs argued a wide variety of damages:
 - Increased risk of identity theft.
 - Untimely and inadequate notification.
 - Improper disclosure of PII.
 - Invasion of privacy.
 - Decreased value of PII.
 - Anxiety and emotional distress.
 - Overpayment for products.

Plaintiffs Lack Standing

- *In re Barnes & Noble Pin Pad Litigation* (N.D. Ill.):
 - Relying on the U.S. Supreme Court decision in *Clapper v. Amnesty Int'l USA Inc.*, No. 11-1025 (2013), the Court granted Barnes & Noble's motion to dismiss.
 - *Clapper*: Held that private citizens lacked standing to challenge 2008 amendments to the Foreign Intelligence Surveillance Act because they could not show the government had actually spied on them.

Plaintiffs Lack Standing

- *In re Barnes & Noble Pin Pad Litigation* (N.D. Ill.):
 - No proof that an “injury in fact” is “certainly impending.”
 - Speculation of future harm does not constitute actual injury.
 - Even if plaintiffs could prove statutory violations, such violations would be insufficient to establish standing without actual injury.
 - Increased identity theft expenses cannot establish standing for non-imminent harm.
 - Emotional distress insufficient absent any imminent threat to PII.
 - Fraudulent charges were reimbursed.

Plaintiffs Lack Standing

- *Polanco v. Omnicell, Inc. (D.N.J.):*
 - In January 2014, the Court dismissed a class action against three healthcare entities and a vendor retained by these entities.
 - After receiving notice that a laptop was stolen that contained plaintiff's unencrypted Personal Confidential Data (PCI) and Protected Health Information (PHI), plaintiff filed this litigation.
 - Plaintiff alleged that, because she did not receive reassurance from defendants that they would adequately protect plaintiff's information from subsequent losses, plaintiff was forced to seek medical treatment at more distant hospitals and, thus, incur higher costs.

Plaintiffs Lack Standing

- *Polanco v. Omnicell, Inc. (D.N.J.)*:
 - Applying *Clapper v. Amnesty Int’l USA Inc.*, No. 11-1025 (2013), the Court held:

“ . . . [plaintiff] has prophylactically spent money to ease her fears of a future loss of her PII and PHI . . . and therefore made an independent decision to seek treatment elsewhere. [Her] decision to do so was based entirely on her speculation that her PII or PHI would be ‘lost’ again by Defendants. Therefore, her assertion is one that claims injury for expenses incurred in anticipation of future harm, and is not sufficient for purposes of establishing Article III standing.”

Plaintiffs Lack Standing

- *Galaria v. Nationwide Mut. Ins. Co. (S.D. Ohio)*:
 - In February 2014, the Court granted plaintiffs' motion to dismiss the case because plaintiffs did not have standing to sue Nationwide.
 - The Court held that plaintiffs' claimed injuries (an increased risk of identity theft, the costs to mitigate that increased risk, the loss of privacy and deprivation of the value of plaintiffs' personally identifiable information) were not sufficient to satisfy the requirements of Article III standing.

Plaintiffs Have Standing

- *Harris v. comScore* (N.D. Ill.):
 - Plaintiffs alleged that defendants improperly obtained and used personal information after consumers downloaded and installed company's software.
 - comScore's data collection violated the User License Agreement and the Downloading Statement.
 - Court found standing based upon statutory damages available under the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act and the Stored Communications Act.

Plaintiffs Have Standing

- *Robins v. Spokeo, Inc. (9th Cir.)*:
 - Plaintiff filed complaint alleging that Spokeo violated the Fair Credit Reporting Act by publishing inaccurate personal information about him.
 - District Court granted motion to dismiss because plaintiff failed to prove an injury-in-fact and, thus, did not establish standing.
 - The Ninth Circuit Court of Appeals reversed the District Court’s decision and held that “the statutory cause of action [FCRA] does not require a showing of actual harm when a plaintiff sues for willful violations.”

Plaintiffs Have Standing, But Have Not Suffered Economic Damages

- *In re: Sony Gaming Networks and Customer Data Security Breach Litig.* (S.D. Cal.):
 - Hackers accessed the personal information of millions of Sony’s customers.
 - Based upon plaintiffs’ allegations in their original complaint, the Court found that plaintiffs did not have standing.
 - After filing an amended complaint, on January 21, 2014, the Court found that plaintiffs’ allegations “that their personal information was collected by Sony and then wrongfully disclosed . . . was sufficient to establish standing at this stage.”

Plaintiffs Have Standing, But Have Not Suffered Economic Damages

- *In re: Sony Gaming Networks and Customer Data Security Breach Litig.* (S.D. Cal.):
 - The Court held that plaintiffs “plausibly alleged a ‘credible threat’ of impending harm” and that plaintiffs were not required to allege that their data was actually accessed by a third party.
 - Although plaintiffs overcame the standing hurdle, the Court dismissed 43 of 51 of plaintiffs’ counts (including breach of contract and negligence claims) for failure to allege any actual economic harm.

Plaintiffs Have Standing, But Have Not Suffered Economic Damages

- *In re: Sony Gaming Networks and Customer Data Security Breach Litig.* (S.D. Cal.):
 - The Court allowed claims under consumer protection statutes to proceed:
 - e.g., unfair competition, false advertising, deceptive and unfair trade practices.
 - Claims mainly based upon alleged misrepresentations regarding “reasonable security” and “industry-standard encryption.”
 - Misrepresentations caused plaintiffs to pay more for product than if accurately described.
 - The elements of statutory causes of action are different than the ones required for common law claims.

Plaintiffs Have Standing, But Have Not Suffered Economic Damages

- *Moyer v. Michaels Stores, Inc. (N.D. Ill.):*
 - In July 2014, although the Court found that plaintiffs had standing, the Court dismissed a class action because plaintiffs could not show any economic damages.
 - “The elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing.”
 - However, the Court found that the increased risk of identity theft did not constitute actual monetary damages as required by consumer fraud statutes.

Scott L. Vernick
215.299.2860
svernick@foxrothschild.com

