Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 10 >>> OCTOBER 2015

The Evolution of Data Breach Litigation in the United States: What's Happening and What's Ahead

By Rajesh De, John Nadolenco and Evan Wooten, of Mayer Brown LLP.

Ever since the high-profile U.S. data breaches of the 2013 holiday season, businesses and legal prognosticators have wondered what courts will do with the many data breach lawsuits that followed. Litigation necessarily lags behind business and technology, even though lawsuits are often filed within days of a reported breach. Cases stemming from the late 2013 data breaches are only now reaching the U.S. Federal Courts of Appeal, such as the Seventh Circuit's July 2015 decision in *Remijas v. Neiman Marcus Group.*[1]

It is tempting to think the law of data breach is only now developing or began developing only in late 2013. In fact, just as businesses have been dealing with threats to data security for decades, U.S. courts have been grappling with data breach cases for nearly as long.

To truly understand data breach case law, businesses and practitioners must go back to the early cases and trace the evolution through to more recent developments. In this way, certain recent cases, such as *Neiman Marcus*, are best seen not as a change in law, but as a deviation from traditional data breach litigation fact patterns.

Early Cases Featured Repeated Fact Patterns

For many people, the term "data breach" calls to mind a cyberattack by hackers or foreign intelligence operatives, but the term has never been so limited.

Early data breach cases in the United States involved repeated fact patterns: Rogue employees would make off with company data for their personal use; faithful employees would leave company laptops unattended in hotel rooms or cars, to be snatched up by thieves; and rival companies would engage in corporate espionage.

These events led to litigation in a variety of forms: consumer class actions, employee class actions, shareholder derivative suits, insurance litigation, and lawsuits by and against third parties, such as an accused employee or credit card companies made to replace cards and reimburse fraudulent charges.

State and federal regulators, like the U.S. Federal Trade Commission, the U.S. Federal Communications Commission and state attorneys general, also bring public enforcement actions in the wake of data breaches.

In the consumer context, courts confronting the traditional fact patterns recognized that, while stolen data often contained personal consumer information, the

object of the theft frequently was confidential business information or the laptop itself. More often than not, there was no indication the thieves had made any use of the personal consumer data contained on stolen laptops or compromised servers.

Certain recent cases, such as *Neiman Marcus*, are best seen not as a change in law, but as a deviation from traditional data breach litigation fact patterns.

As a result, U.S. courts have traditionally dismissed consumer suits, reasoning that plaintiffs could not allege or prove an essential element of most every claim under U.S. law: *actual harm*. Plaintiffs alleged numerous theories of recovery, such as breach of consumer user agreements and privacy policies, negligent failure to safeguard consumer data, and invasion of privacy. Courts have generally dismissed each of these theories in turn, for numerous reasons: User agreements rarely impose data security obligations, meaning there is no contract to breach; negligence plaintiffs often can recover only for personal or property damage, while the most data breach victims usually allege is economic loss; and invasion of privacy is compensable only if private information is published, among other requirements.

The theories and legal rules differed, but the thrust was always the same: Data breach plaintiffs could not allege that their identities had been stolen or their personal data misused in a way that caused actual harm.

Cases leading up to and following the late 2013 data breaches introduced new variations on the traditional fact patterns: Hackers "skimmed" credit card information from PIN pad readers, for example, and infiltrated computer networks through malware. But though the fact patterns varied, the results were generally the same.

The U.S. Supreme Court's Decision in the *Clapper* Case

The prevailing rule crystallized in a line of cases applying the "case" or "controversy" requirement of the U.S. Constitution, Article III, as interpreted by the U.S. Supreme Court in the 2013 decision, *Clapper v. Amnesty International USA*.[2] *Clapper* was not a data breach case, but rather involved the U.S. Foreign Intelligence Surveillance Act (FISA).[3] U.S. journalists reporting on foreign affairs sued to invalidate 2008 amendments concerning surveillance of non-U.S. persons located abroad. The journalists feared their foreign communications would be surveilled, and some traveled long distances to meet personally with contacts.

The Supreme Court concluded that the threat of potential surveillance was not sufficiently imminent ("certainly impending") to create an actual case or controversy capable of judicial resolution. The journalists' "theory of future injury" was "too speculative" to satisfy Article III, resting on a chain of "highly attenuated" inferences, including that the government would, in fact, target the journalists' contacts, obtain a FISA warrant, and intercept communications. In the Supreme Court's view, the journalists had suffered no concrete injury to compensate.

Courts applying *Clapper* to data breach complaints have generally found that the risk of future identity theft is too speculative to support a lawsuit.

A decision of the Washington D.C. District Court[4] illustrates the prevailing view and a traditional fact pattern: A thief broke into the car of a government contractor's employee and stole the car stereo, GPS, and several data backup tapes that contained personal information on roughly 5 million U.S. military service members and their families. Service members in eight U.S. states sued. But the district court dismissed the lawsuit, explaining that the tapes "could be uploaded onto [the thief's] computer and fully deciphered, or they could be lying in a landfill somewhere in Texas because she trashed them after achieving her main goal of boosting the car stereo and GPS." There was "simply no way to know" what became of the breached data until "the crook [was] apprehended or the data [was] actually used."

Similarly, an Ohio court dismissed claims stemming from a systems hack because the plaintiffs could not allege any actual identity theft, identity fraud, medical fraud, or attempts by the hackers to "phish" for personal information.[5]

And an Illinois court dismissed a skimming complaint, as the plaintiffs could allege only that they made PIN pad purchases, not that their credit card data was compromised.[6]

In each case, the increased risk of identity theft in the future was too speculative to satisfy the Article III standing requirement. As the Ohio court explained: "[H]ow much more likely [data breach plaintiffs] are to become victims than the general public is not the same as . . . how likely they are to become victims" in fact.[7]

Recent Decisions Reach Different Results

However, a few recent decisions have reached different results, in particular, a California district court decision[8] and, more recently, the Seventh Circuit's decision in *Neiman Marcus*. In each case, the defendant company was the victim of a sophisticated, deliberate hack targeting its systems and servers specifically. In the California case, "stolen data had already surfaced on the Internet" and, in the Seventh Circuit case, over 9,000 card members had already suffered fraudulent charges, incurring costs to replace credit cards and monitor for further fraud. Applying *Clapper*, both courts found that the risk of identity theft was substantial ("certainly impending") and the costs incurred were not insignificant ("*de minimis*").

Some have viewed the recent decisions, *Neiman Marcus* in particular, as signaling a shift in data breach case law in the United States. For now, however, those cases remain outliers marked by their unique facts.

The Seventh Circuit emphasized that several thousand card members had already suffered fraudulent charges,

   ISSN 1473-3579

whereas the journalists in *Clapper* had not suffered any actual interception of foreign communications. And the California court explained that the deliberate data hack, which led to consumer data surfacing on the Internet, stood in "sharp contrast" to a laptop theft, where stolen tapes could indeed be lying in a landfill somewhere. Both cases invoked and applied the Supreme Court's decision in *Clapper* — they simply reached different results on the facts presented.

Looking Ahead

What are businesses to make of the recent decisions, then, or the cases that came before?

Most likely, data breach cases will continue to turn on their particular facts. Article III of the U.S. Constitution continues to apply to all cases in U.S. federal court and requires that data breach plaintiffs, like all plaintiffs, articulate concrete harm before maintaining a suit.

Not all data breaches are created equal, and there are many permutations on the spectrum between a random laptop theft and a deliberate criminal hack that results in thousands of fraudulent charges. Recent studies suggest that system malfunction and human error are nearly as common causes of data breach as malicious criminal attacks.[9] Courts may well conclude that the risk of identity theft from a prior breach is not sufficiently imminent unless numerous fraudulent charges already have resulted from a sophisticated and deliberately targeted attack, and, even then, the harm not be sufficiently concrete.

Just as all data breaches are not created equal, plaintiffs have tried to allege many forms of harm. Courts such as the Seventh Circuit have expressed skepticism over claims based on an abstract loss of private information or overpayment for services, and recognized important factual differences in bank reimbursement policies that will affect case outcomes. As the cyber threat evolves and data may be exfiltrated by adversaries for purposes not clearly tied to demonstrable identity theft, courts may be less inclined to assume imminence of real world harm to individual plaintiffs.

Finally, it is important to note that the debate thus far has focused primarily on whether consumers can maintain lawsuits. U.S. courts have yet to address whether and to what extent data breach lawsuits have merit or whether such cases can be maintained as class actions.

Business and legal observers should stay abreast of the continued evolution of data breach case law in the United States.

NOTES

[1] *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015).

[2] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

[3] 50 U.S.C. § 1801 *et seq.*

[4] *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014).

[5] *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014).

[6] *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617 (N.D. Ill. Sept. 3, 2013).

[7] *Galaria*, *supra* note 5, at 654.

[8] *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

[9] Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis 1, 7 (2013), *available at* http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf.

Rajesh De is a Cybersecurity and Data Privacy Partner in the Washington office, John Nadolenco is a Litigation and Dispute Resolution Partner in the Los Angeles office and Evan Wooten is a Litigation and Dispute Resolution Associate in the Los Angeles office, of Mayer Brown LLP. They may be contacted at rde@mayerbrown.com, jnadolenco@mayerbrown.com and ewooten@mayerbrown.com.