Bloomberg BNA

Privacy and Security Law Report®

Expect to See More Data Breach Class Actions in the Eleventh Circuit



BY MICHAEL R. PENNINGTON, JOHN E. GOODMAN AND CAMERON ELLIS

A divided panel of the U.S. Court of Appeals for the Eleventh Circuit recently issued what is likely to be an irresistible invitation to would-be class counsel to file their data breach class actions in federal courts in the Southeast. The invitation comes in the form of an opinion in *Resnick v. AvMed Inc.*[1] The decision allowed plaintiffs to survive dismissal of their data breach class actions without having to plead any specific facts actually tying their identity theft damages to the data breach at issue.

Data breaches occur when personally identifiable information (PII), typically held by a business entity in confidence, makes its way into the hands of a third party. Such PII can range from names and addresses to Social Security numbers, and from financial account numbers to personal health information. Data breaches can be intentional (hackers, stolen laptops or devices, etc.) or unintentional (system glitches, employee negligence, etc.). Human error and glitches are the root cause of most data breaches. But those caused by malicious hacking and other deliberate misdeeds may be increasing.[2]

Generally, data breach class action plaintiffs have struggled to demonstrate actual harm stemming from a company's lapse in data security. In recent years, thanks to U.S. Supreme Court decisions such as *Bell Atlantic Corp. v. Twombly*[3] and *Ashcroft v. Iqbal*,[4] federal courts have been insisting that plaintiffs plead causation and other elements of a claim with greater specificity. The now-prevailing standards require plaintiffs to do more than simply state the elements of the claim, causation and liability in conclusory fashion, and instead require complaints to allege a detailed set of facts establishing a plausible factual and legal basis to find the named defendant liable for the injury alleged. *Resnick* seems to buck this trend and instead allow data breach class actions to proceed without alleging any specific factual link between a data breach and a plaintiff's identity theft or other actual injury.

In *Resnick*, laptops owned by a home health care company were stolen by unidentified thieves. The laptops had unencrypted customer data such as the names, addresses, and Social Security numbers of customers. Ten and 14 months, respectively, after the laptop thefts, the named plaintiffs suffered identity thefts that involved the same type of information. They filed suit against AvMed under a variety of theories. The plaintiffs pleaded no facts showing that the identity thieves obtained their names, addresses, and Social Security numbers from the stolen laptops, as opposed to some

[1] *See Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (11 PVLR 1413, 9/17/12). The decision is available at http://op.bna.com/hl.nsf/r?Open=mapi-8xzpsx.

Michael R. Pennington and John E. Goodman are partners, and Cameron Ellis is an associate, in the Class Actions Practice Group at Bradley Arant Boult Cummings LLP in Birmingham, Ala.

[2] *See* Ponemon Institute LLC, *2011 Cost of Data Breach Study* (March 2012) 11 PVLR 562, 3/26/12.

[3] *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007).

[4] *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

 ISSN 1538-3423

other source. Instead, they simply alleged that they had always been careful to safeguard their personally identifiable information and never were victims of identity theft until 14 months after AvMed's laptops were stolen.

Nevertheless, the Eleventh Circuit reversed the trial court's dismissal of the complaint and allowed the class action to proceed without requiring any greater showing of causation. While correctly recognizing that it was not, under *Twombly* and *Iqbal*, bound to accept as true the conclusory allegation that the defendant was the cause of plaintiffs' identity thefts, the court concluded that merely alleging that plaintiffs' names, addresses, and Social Security numbers were on the stolen laptops and the type of data used to perpetrate the identity theft incidents brought the case against this specific defendant ''from the realm of the possible into the plausible.''[5] The court did not find persuasive the argument, pointed out by Judge William H. Pryor Jr., in his dissent, that ''vast numbers of individuals, businesses, and governmental bodies possess our sensitive information, e.g., our names, social security numbers, health information, and other personal data.''[6] Judge Pryor explained that the issue is not whether identity thieves used plaintiffs' personal information; they unquestionably did. Instead, the question is whether the complaint provided any plausible basis to conclude that the identity thieves even had any connection whatsoever with the laptop thieves, and whether the identity thieves who actually inflicted the harm upon the plaintiffs got their access to plaintiffs' personal information from the defendant or elsewhere.[7]

Resnick veers toward turning a data breach defendant into an insurer of the persons whose data it holds, without regard to whether it can be alleged or shown that its breach in fact caused the subsequent harm of which plaintiff complains. There are no facts pleaded in the *Resnick* complaint to show that AvMed's laptop theft incident had any causal role at all in plaintiff's identity theft. The *Resnick* plaintiffs surely had business relationships with numerous entities over the past several years that resulted in those entities having plaintiffs' names, addresses, and Social Security numbers. Many or even most of those entities may have suffered a known or unknown data breach over the last few years as well. *Resnick* seems tantamount to a *de facto* form of joint and several liability for businesses that suffer a data breach of commonly held customer information—anyone can be sued for the sins of all, without any burden of the defendant to plead facts demonstrating which breach is actually the cause of plaintiff's loss.

The practical implications of *Resnick* are potentially quite significant. Once a class action survives dismissal in federal court, it will generally proceed toward the class certification stage. The specter of class certification, with only a rarely granted discretionary appeal of the class certification issue before trial and final judgment in federal court, places tremendous pressure upon defendants to settle, not only because of their potential exposure, but also because of the tremendous expense that class action discovery, motion practice, and expert witness practice frequently entails. Not surprisingly, many data breach class actions that survive dismissal result in class settlements. In recent years, the University of Hawaii (11 PVLR 237, 2/6/12), TD Ameritrade (10 PVLR 1378, 9/26/11), Netflix, Wellpoint, Certegy (7 PVLR 464, 3/31/08), Heartland Payment Systems (11 PVLR 549, 3/26/12), and Stratfor defendants are just some of the data breach class action defendants who have succumbed to the settlement pressure.

So what can a company do to minimize its exposure to data breach class actions? Companies that do business with customers in the Eleventh Circuit cannot avoid the implications of *Resnick* once a data breach has occurred, but they can take steps in advance to minimize the risk of a data breach occurring, and to mitigate the company's exposure in the event a data breach occurs.

The nature of the company's business, the type of information at issue, and the location of customers and information involved can have a significant effect on the company's obligations with respect to customer data and the company's obligations in responding to a data breach. For example, in the FTC's recent case against PLS Financial Services Inc. (11 PVLR 1655, 11/12/12), which involved financial information associated with payday lending and check cashing transactions, the FTC relied primarily upon the Gramm-Leach-Bliley Safeguards Rule and Privacy Rule and the FTC Disposal Rule, but also invoked the FTC Act generally, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transactions Act. But health care providers may be much more concerned with the obligations imposed by the Health Insurance Portability and Accountability Act. And whatever federal statutes may be applicable, businesses must also comply with widely varying state laws that are often invoked by private plaintiffs and state attorneys general, such as the ''Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth,'' regulations found at 201 Mass. Code Regs. 17.00 and issued pursuant to the Massachusetts Consumer Protection Act, Mass. Gen. Laws. ch. 93A, § 2. Forty-six states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have enacted security breach notification laws of one kind or another.[8] Still, there are some general rules to go by in minimizing data breach exposure.

The first rule of thumb for minimizing exposure from data breaches is to encrypt sensitive customer data both in transmission and in all forms of storage. HIPAA and some state statutes have explicit ''safe harbors'' for encrypted data, while others do not. But it can hardly be doubted that following industry ''best practices'' encryption standards is very helpful in minimizing both reporting requirements and litigation exposure in the event of a data breach. Identifying all types of customer data the company has and mapping exactly how the data are stored and transmitted is a critical step in the process. Mobile devices should be password-protected on a mandatory basis company-wide. Companies must also ensure any vendors or contractors with access to customer data are also in compliance with the applicable state and federal statutes.

While the requirements of any applicable state or federal statute always control, many businesses currently

[5] *Id.* at 1327.
[6] *Id.* at 1332.
[7] *Id.*

[8] *See, e.g.*, National Conference of State Legislatures, *State Security Breach Notification Laws* (Aug. 20, 2012), http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (collecting such statutes).

  PVLR ISSN 1538-3423

regard ISO Standard 17799/27001 as a default ''best practices'' standard for data encryption. The safest course is to make data encryption and password protection the default, so that employees have to take special steps to keep customer data from being encrypted and mobile devices from being password protected. This concept is known as ''privacy by design.''

A second important way of minimizing exposure in the event of a data breach is to keep sensitive data no longer than necessary, and then dispose of the data promptly, properly, and securely. Again, data retention and disposal rules vary depending on the type of data at issue and which state and federal laws apply to the transactions at issue.[9] Care should always be given to comply with the obligation to preserve data potentially relevant to pending or imminent litigation. Far too many companies keep customer data indefinitely simply by virtue of inertia. This not only multiplies the company's exposure to data breach liability; it also increases the burdens of electronic discovery and the overall cost of information systems maintenance and infrastructure.

Disposing of customer information that has fulfilled its purposes as soon as the law allows is a critical part of any sound document retention policy. In implementing such a policy, it is important to remember that many devices other than computers contain ''drives,'' such as printers, copiers, scanners, smartphones, media players, etc. While state and federal disposal laws and regulations applicable to a given data and media set are of paramount importance, examples of commonly cited ''best practices'' for data disposal include the following:

- destroy paper records by shredding or otherwise rendering any personal information on such records unreadable and undecipherable;
- at a minimum, take steps to completely overwrite deleted personal information on hard drives, disks, or tapes if they are to be reused, and if they are to be destroyed, abrade and shred disk surfaces and degauss or burn tape media (Commonly referenced data disposal standards include DoD 5220.22, ISO 27001 and ISO 9002.);
- undertake meaningful due diligence on any company with which you contract to supply data disposal services (including a review of audits of the company's operations, requiring certification by a recognized trade association or similar third party, and a review of the company's information security policies); and
- require that any data destruction be conducted on site.

Companies also must have a plan in place for responding to data breaches, should they occur. This includes understanding notification requirements under state and federal law for every type of consumer data kept by the company. Even when notifications are not required, they might help prevent identity theft and other actual injury to customers. Some courts have also found that offering pre-purchased identity theft protection and credit monitoring services for affected customers can prevent ''fear of future identity theft'' from being an actual injury in a data breach class action.[10]

In light of *Resnick*, it is clear that companies must ensure they take all appropriate and required steps to prevent data breaches and the loss of customer information. It is equally important to have the right mitigation plans in place if a breach is discovered. If courts follow the Eleventh Circuit's lead, data breach class actions will be much more likely to survive early dismissal in the future, and even more aggressively pursued by would-be class counsel than they already are.

---

[9] *See, e.g.*, National Conference of State Legislatures, *Data Disposal Laws* (June 22, 2012) http://www.ncsl.org/issues-research/telecom/data-disposal-laws.aspx (collecting various state statutes on data disposal).

[10] *See, e.g.*, *Hammond v. The Bank of New York Mellon Corp.*, No. 08-6060 (S.D.N.Y. June 25, 2010). Full text of the decision is available at http://op.bna.com/pl.nsf/r?Open=dapn-92pjmg.