METROPOLITAN
CORPORATE
COUNSEL®

FEBRUARY 2016 WWW.METROCORPCOUNSEL.COM

Courts Send Mixed Messages on Standing for Plaintiffs in Data Breach Litigation

By Devin Chwastyk / McNees Wallace & Nurick LLC

New decisions from two federal courts may allow defendants in data breach class action litigation to breathe somewhat easier, following a run of adverse decisions last year. These decisions illustrate an emerging trend of district courts dismissing such privacy claims for lack of standing. Those decisions run directly counter to some court rulings last year that made it easier for plaintiffs to state a claim where their information has been compromised. These competing trends may bring data breach litigation to the U.S. Supreme Court in the near future.

Judicial decisions in 2015 brought plenty of bad news for companies that collect and store personally identifiable information of customers and employees. As noted in the November 2015 issue of *Metropolitan Corporate Counsel*, last year saw the Seventh Circuit rule that victims of data breaches may have their day in court even where they suffered no actual fraud losses as a result of their information being exposed. In that case against Neiman Marcus, the court found that efforts to prevent possible future fraud, such as credit monitoring, are sufficient as damages to provide plaintiffs with standing to sue.

Perhaps equally as troubling from a defense perspective, the U.S. District Court for Minnesota last year certified a data breach class action for the first time. The court allowed financial institutions to proceed as a class against Target for losses incurred when hackers accessed payment card information belonging to millions of customers.

Meanwhile, the Third Circuit Court of Appeals last year found that the Federal Trade Commission (FTC) had authority to bring enforcement actions against companies that are victims of hacking attacks, on the basis that corporate security failures amount to unfair and deceptive trade practices.

The new year, however, opens with some cause for optimism for organizations threatened by the risk of data exposure litigation. Two recent federal court decisions illustrate a trend to dismiss cases where the individuals affected cannot show they suffered actual financial harm due to fraud on their accounts. The contrast of these two decisions with the pro-plaintiff rulings from last year may indicate potential for circuit split that would allow a data breach case to reach the U.S. Supreme Court.

Competing trends may bring breach litigation to the Supreme Court in the near future.

The federal court for the Eastern District of New York issued one decision in favor of data breach defendants in the final days of 2015. In *Whalen v. Michael* [sic] *Stores, Inc.*, the Michaels chain of arts and crafts stores had been sued after hackers used malware to retrieve customers' credit and debit card information from its systems. The complaint alleged that the class representative had experienced two attempted fraudulent charges to her credit card, but those transactions were not approved, and she cancelled her card thereafter. She further alleged damages in the form of lost time and money associated with credit monitoring and card replacement, and potential future harm arising from the continuing risk of identity theft once her information had been exposed to hackers.

The Michaels court held that class plaintiffs lack standing when they assert only the potential risk of future harm. First, the court noted that Whalen had not suffered any unreimbursed charges to her accounts. Even if the attempted fraudulent transactions had been processed, the court noted, she would have been reimbursed under the zero-fraud liability terms set by card issuers. Next, the court rejected as cognizable damages the alleged loss of time and money associated with credit monitoring, holding that plaintiffs may not manufacture standing by their efforts to avoid potential future harm.

In a direct departure from last year's analysis by the Seventh Circuit in *Neiman Marcus*, the New York court in *Michael* ruled that the risk of future identity theft is not sufficient to establish standing to sue. Relying on the U.S. Supreme Court's now familiar Clapper standard (which was announced in a case challenging government wiretaps), the court held such risk must be imminent and substantial rather than merely possible to allow a lawsuit to overcome a motion to dismiss.

Likewise, the U.S. District Court for Minnesota (the same court that last year certified the *Target* class of financial institution plaintiffs) started 2016 by dismissing, for lack of standing, consumer claims against a retailer. In the SuperValu class action, 16 named plaintiffs brought claims alleging the grocer defendants had negligently failed to protect the plaintiffs' payment card information after hackers accessed the defendants' systems.

The *SuperValu* decision, like the *Michael* ruling, dismissed the putative class action for lack of standing because none of the named class plaintiffs had alleged that they suffered actual fraud losses as a result of the breach. The court was especially troubled by the numerous variables upon which the plain-

Devin Chwastyk
Chair of the Privacy & Data Security group at McNees Wallace & Nurick LLC.
dchwastyk@mwn.com

McNees

tiffs' allegations of future harm rested, which included whether hackers indeed still had possession of the stolen personal information, and whether those hackers would in the future use the particular card data belonging to the named class plaintiffs.

Of note, the *SuperValu* decision came from the same court that allowed the *Target* data breach litigation to proceed over motions to dismiss filed earlier in that case. The distinguishing factor appears to be the artful pleading of the plaintiffs' lawyers in *Target*, who suggested that actual fraud losses had occurred that may not have been remedied by the zero-fraud protection of consumers. In contrast, the complaint in *SuperValu* made clear that only one of the 16 plaintiffs had seen an actual fraudulent transaction on their payment card, and that transaction had been cancelled, so there had been no real financial injury to that plaintiff.

Although the *Target* and *Neiman Marcus* decisions may provide adequate support for plaintiff's counsel to continue to bring class actions whenever a data breach becomes public, the *Michael* and *SuperValu* decisions are illustrative of a predominant trend: Most federal courts are dismissing such claims in the absence of actual fraud losses, based on the U.S. Supreme Court's decision in *Clapper*. At least a dozen district courts have dismissed putative data breach class actions for lack of actual injury since 2014.

Privacy lawyers now await an appellate court ruling affirming this trend in the district courts. A federal circuit court decision that data breach claims cannot be maintained based on the threat of future fraud against the plaintiffs would stand in direct contrast to the Seventh Circuit's ruling in *Neiman Marcus*. This would set up a circuit split, which might lead to a grant of certiorari from the U.S. Supreme Court. The U.S. Supreme Court then would be left to decide whether the reasoning of its *Clapper* decision has been properly applied in the context of data breach litigation, and perhaps, to decide whether data breach claims will have a future at all.