Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Privacy Litigation Developments You May Have Missed

By **Allison Grande**

Law360, New York (January 26, 2016, 4:52 PM ET) -- With privacy attorneys focusing on headline-grabbing developments such as the landmark settlements in the Target and Wyndham data breach suits, several important developments have flown under the radar, including a case that introduces a new liability for information security companies and a pair of court rulings that complicate plaintiffs' standing in data breach cases.

Here, Law360 recaps major privacy and data security case law developments that you may have overlooked.

Trustwave Targeted by a Client

Las Vegas-based casino operator Affinity Gaming LLC on Dec. 24 took aim against cyberforensics firm Trustwave Holdings Inc., launching a suit accusing the company of failing to investigate, diagnose and help remedy Affinity's 2013 data breach.

Trustwave's allegedly false representations that it had conducted a thorough investigation and removed the threat caused Affinity to hire a second data security consulting firm, Mandiant, which found that the malware was still in the system and that Trustwave's work had been "woefully inadequate," according to the complaint.

While data breach targets typically face an onslaught of litigation from parties including consumers, financial institutions and shareholders following a security incident, having the compromised business turn the tables and sue the company it hired to help it recover from the breach is a relative novel approach, and one that is likely to make security firms think more carefully about their work.

"It does put some pressure on companies to strongly evaluate the claims that vendors are making, and it could have the perhaps unintended consequence of making vendors in this context more cautious overall about their conclusions, which will make it harder for their clients to make decisions about what has happened with a breach," Wiley Rein LLP privacy practice chair Kirk Nahra said.

Trustwave has faced legal scrutiny over its cyberforensics work in the past, but the fallout thus far has come from those affected by the breach.

The firm was named as a defendant in putative data breach class actions that financial institutions launched against Target Corp. and that a South Carolina resident brought against the state's tax

department. Both suits accused the breached entity as well as Trustwave of failing to take steps to prevent the intrusions, but the data security firm shook both suits.

"A forensics examination is not as simple as many companies would like to believe," Shook Hardy & Bacon LLP data security and privacy practice co-chair Al Saikali said. "Unlike the medical world, where a doctor may already know where the infection resides and how to treat it, the cause of a data breach can often be very difficult to find, and it can migrate quickly and, though seemingly removed, return easily."

While it's still too early too tell if Affinity has enough to prevail in its lawsuit — especially given that Trustwave, which has publicly denied the allegations, has yet to present its side in court — attorneys noted that while forensics firms may seem like attractive targets to include in the post-breach litigation melee moving forward, factors such as the failure of the breached entity to give the firm the entire story and strong limitation of liability language in contracts may make success on the merits difficult.

"Generally, forensic firms are easy targets, often with deep pockets, [and] these lawsuits and threats of lawsuits are an easy way for breached companies to blame and recover money from someone else," Saikali said. "[But] companies should think twice about the repercussions of blaming their loses on forensics firms."

Affinity Gaming is represented by Jonathan L. Missner and Robert B. Gilmore of Stein Mitchell Cipollone Beaton & Missner LLP and I. Scott Bogatz of Reid Rubinstein & Bogatz.

Counsel information for Trustwave was not immediately available.

The case is Affinity Gaming v. Trustwave Holdings Inc., case number 2:15-cv-02464, in the U.S. District Court for the District of Nevada.

Breach Victims Get Boost in Massachusetts

In a reversal of fortune for data breach plaintiffs, a Massachusetts Superior Court judge in November shot down Boston Medical Center Corp.'s motion to dismiss a putative class action over the exposure of patient medical records, even though the plaintiffs had alleged only that the data had been made publicly available and not that any unauthorized parties had viewed or misused the information.

The decision went against a long line of dismissals handed down in data breach suits by federal courts in the wake of the U.S. Supreme Court's landmark 2013 ruling in Clapper v. Amnesty International USA, which established that plaintiffs need to prove they have suffered actual harm or a certainly impending injury to satisfy standing requirements under Article III of the U.S. Constitution.

"Given the nature of the type of information at issue, the decision isn't actually all that surprising and is consistent with a trend of courts beginning to be a little more sophisticated about the nature of information at risk and treating data such as medical information different from data such as payment card information," Mintz Levin Cohn Ferris Glovsky & Popeo PC member Kevin McGinty said.

While it may be hard for plaintiffs outside of Massachusetts to cite the decision in any persuasive way, given its posture as a Superior Court opinion that rests on state and not federal law, that doesn't mean they won't at least try, attorneys noted.

"When plaintiffs are trying to make a case, they will seize anything that will help them," McGinty said.

The case is Walker et al v. Boston Medical Center Corp., case number 2015-1733-BLS, in the Massachusetts Superior Court.

Familiar Story in Michaels Breach

In contrast to the Massachusetts case, a New York federal judge on Dec. 28 reached a wholly different ruling in dismissing without prejudice a proposed class action against arts and crafts retailer Michaels Stores Inc. over an intrusion announced in 2014 that impacted nearly 3 million payment cards.

Citing the Clapper decision, the judge rejected named plaintiff Mary Jane Whalen's argument that she had standing to pursue her claims, since there were no unauthorized fraudulent charges on her card.

The decision follows a lengthy trend of actions over credit card breaches at businesses such as eBay Inc. and P.F. Chang's China Bistro Inc. being tossed at the motion to dismiss stage, and has already been cited by Barnes & Noble Inc. in its effort to convince an Illinois federal court to nix consolidated class actions stemming from a security breach that exposed PIN pad devices at dozens of stores in 2012.

"The Michaels decision reinforces the notion that there really isn't an actionable injury for consumers in payment card cases, especially since it's really impossible for someone to steal a person's identity with credit card data and consumers are made good on fraud losses," McGinty said.

Whalen is represented by Glancy Prongay & Murray LLP, Siprut PC and Lite DePalma Greenberg LLC.

Michaels is represented by James D. Arden, Edward McNicholas and Michelle Hartmann of Sidley Austin LLP.

The case is Whalen v. Michaels Store Inc., case number 2:14-cv-07006, in the U.S. District Court for the Eastern District of New York.

Calif. Court Weighs Businesses' Privacy Rights

A California appeals court drew a line in the sand on Dec. 11, when it concluded that corporations don't enjoy the right to privacy afforded to "people" under Article I of the state constitution.

However, the appellate court didn't stop there, reaching the additional finding that corporations do have a right to privacy that is subject to a balancing test, which the panel used to reject petitioner SCC Acquisitions Inc.'s argument it did not have to comply with requests for documents made by creditor Western Albuquerque Land Holdings Inc. as part of its efforts to enforce a $47 million judgment against SCC Acquisitions.

"The holding in this case that corporations have no constitutional right of privacy is a bit of a curate's egg," Allen Matkins Leck Gamble Mallory & Natsis LLP partner Keith Paul Bishop said. "Creditors don't want debtors asserting privacy rights to frustrate collection efforts. At the same time, corporations will want to assert privacy rights to frustrate attempts by claimants to gain access to information to use against the corporation in litigation."

Bishop pointed out that other courts of appeal in the state have reached a different conclusion than the one in the instant matter, making it likely that the question of whether corporations do have a

constitutionally protected right to privacy could soon find its way to the California Supreme Court.

The case is SCC Acquisitions Inc. v. The Superior Court of Orange County, case number G050546, in the Court of Appeal of the State of California, Fourth Appellate District.

'Roving Warrant' Law Takes Center Stage in NJ

The New Jersey Supreme Court is currently grappling with the hot-button issue of police surveillance in a case challenging the constitutionality of the state's "roving warrant" law that allows police to wiretap phones that are not identified in the warrant application in order to gather time-sensitive information.

"Traditionally, the New Jersey Supreme Court has been at the forefront in defining privacy interests, often departing from its federal counterparts," said Fernando Pinguelo, the chairman of the cybersecurity and data protection group at Scarinci Hollenbeck LLC.

The U.S. Supreme Court in recent years has taken on similar warrantless electronic surveillance issues, ruling in 2014's Riley v. California that a warrantless search of a cellphone during an arrest is a Fourth Amendment violation and in 2012's U.S. v. Jones that GPS vehicle tracking constitutes a "search" for the purposes of the Fourth Amendment.

During oral arguments in the New Jersey case on Dec. 2, Hector Feliciano's attorney took issue with the fact that investigators can wiretap unidentified phones under the state's Wiretapping and Electronic Surveillance Control Act as long as they can prove exigent circumstances later, while the state countered that the government isn't out to violate people's privacy rights with the law, setting the stage for a ruling that will help to further sketch the bounds of law enforcement's electronic surveillance authority.

"As with many other privacy issues brought to bear in the criminal context, the ruling here will likely implicate broader privacy concerns concerning cellphone usage and surveillance and further solidify the court's practical approach to applying rapidly changing technologies to thorny fact patterns," Pinguelo said. "It will also test the limits of New Jersey's Constitution in the wake of federal court decisions that have interpreted similar provisions and found them to be constitutional."

New Jersey Assistant Deputy Public Defender Elizabeth C. Jarit argued the case for Feliciano.

Deputy Attorney General Steven A. Yomtov argued the case for the state.

The case is State of New Jersey v. Hector Feliciano, case number 074395, in the New Jersey Supreme Court.

--Editing by Katherine Rautenberg and Catherine Sum.