Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Equifax's Massive Data Breach To Spur Uncharted Legal Woes

By **Allison Grande**

Law360, New York (September 8, 2017, 10:20 PM EDT) -- Equifax is already facing at least two putative class actions less than a day after disclosing a cyberattack that potentially impacted 143 million consumers' personal data, and attorneys say the unprecedented scope of the breach is likely to offer both advantages and drawbacks to consumers as they fight to prove that they were harmed and that controversial arbitration clauses shouldn't apply.

As has become customary in the wake of headline-grabbing data breaches, consumers in Georgia and Oregon late Thursday sued Equifax just hours after the credit reporting giant announced that hackers had accessed roughly 143 million U.S. consumers' names, Social Security numbers and other sensitive personal information between May and July.

Both suits fault Equifax for, as the Georgia plaintiffs put it, "gargantuan failures" to secure and safeguard consumers' personally identifiable information. The Georgia action additionally alleges that Equifax, which learned about the breach on July 29, kept consumers in the dark for too long.

"This is probably the worst breach ever of a nongovernment organization," said Michael Gold, co-chair of the privacy, information management and data protection group at Jeffer Mangels Butler & Mitchell LLP.

While larger breaches have been reported in the past — most notably, a pair of infiltrations at Yahoo that impacted usernames, hashed passwords and other account data tied to at least 1.5 billion accounts — those incidents didn't involve the type of highly sensitive, difficult-to-replace, crown jewels of personal information at issue in the Equifax hack, which is estimated to have affected more than 4 in every 10 Americans, attorneys noted.

The unprecedented nature of the incident is likely to present new challenges and questions in the courtroom, where plaintiffs suing over similar large-scale data breaches at Yahoo, Target, SuperValu, Michaels Stores, CareFirst and P.F. Chang's have had mixed results in trying to prove that the incident caused them the actual harm necessary to establish Article III standing.

"Given the scope of the information potentially compromised, it remains to be seen how courts will handle the likely class action lawsuits," said Cynthia Larose, chair of Mintz Levin Cohn Ferris Glovsky & Popeo PC's privacy practice.

While Equifax has taken what it called the "unprecedented step" of offering every U.S. consumer its

TrustedID Premier credit monitoring and identity theft protection service for free for a year, "compromises of SSN and driver's license numbers — in combination with everything else that Equifax assembles on consumers — are more difficult to 'remedy' by a 12-month offer of credit monitoring," Larose said.

"Credit monitoring will only alert consumers to new account fraud — and is not useful for identity theft, which is the main concern with the combination of information compromised," Larose added. "You cannot get a new SSN, and unless Equifax will affirmatively tell consumers whether a driver's license has been compromised, most states will be reluctant to issue a new driver's license."

On the other hand, the vast scale of the incident could also undermine plaintiffs' standing arguments by making it difficult to prove definitively that the harm they allege was actually a result of the Equifax breach, according to Seth Berman, who leads Nutter's privacy and data security group.

"After all, with 143 million records breached, many of the consumers affected in this incident will have already been the victim of identity theft from other incidents, making it very difficult to determine who specifically was harmed by this breach," Berman said.

The size and breadth of the breach could also make calculating damages challenging, said Gretchen Ruck, director of consulting firm AlixPartners.

"Given that it's the first breach of its type and affects so many people, it will be interesting to see how it turns out and how courts are going to approach it, given that the damages could be astronomical," Ruck said.

The plaintiffs in the Georgia suit filed Thursday included a laundry list of injuries that they have or are likely to suffer as a direct result of the breach. Those include costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts, damages arising from the inability to use their PII and access to their account funds, the loss of their privacy, and potential fraud and identify theft posed by their PII being placed in the hands of criminals.

The Oregon case alleges that at least one plaintiff had already purchased third-party credit monitoring services and requested that Equifax "provide fair compensation in an amount that will ensure every consumer harmed by its data breach will not be out-of-pocket for the costs of independent third-party credit repair and monitoring services."

While Equifax is likely to push back hard at these assertions, attorneys noted that both the richness and quantity of data compromised could spur courts to be sympathetic to plaintiffs and find the alleged injuries to be more than just speculative.

"With respect to litigation, bad facts can make bad law," said Donna Wilson, chair of Manatt Phelps & Phillips LLP's privacy and data security practice and co-chair of its financial services group. "Courts may take this as an opportunity to push the bounds of standing and injury requirements, class certification standards, and damages inquiries within the data breach context."

Another issue that is likely to come up during court proceedings that have yet to be filed is what legal footing Equifax has to include a class action waiver in the terms that consumers agree to when they sign up for its free credit monitoring and identity theft protection service, thereby requiring participants to submit to arbitration.

"Right now, Equifax is getting terrible publicity in the court of public opinion for these terms," said VLP Law Group LLP partner Melissa Krasnow. "The issue is likely to be brought to the court, and it will be interesting to see how the court deals with the fairness aspect of it in terms of how Equifax is implementing this credit monitoring offering and whether people are really agreeing to the terms and whether they are enforceable."

New York Attorney General Eric Schneiderman was among the critics who slammed this provision Friday, saying on Twitter that the language was "unacceptable and unenforceable" and revealing that his office had already contacted Equifax to demand its removal.

"With something of this magnitude, it's doubtful whether an arbitration provision like this is going to be able to swamp the ability of data subjects to bring claims in court," Gold said.

Attorneys say that the Equifax breach and its resulting publicity should act as a wake-up call to companies in every sector, given not only its magnitude but also the type of company that Equifax is.

"This is a watershed moment," said Brenda Sharton, chair of Goodwin Procter LLP's privacy and cybersecurity practice and its business litigation practice. "When you have a company in the cybersecurity ecosystem, that you normally call when there is a breach, it is a little jarring for people for it to suffer a breach. It is a reminder that no company is immune."

According to Sharton, the breach offers several takeaways, including the importance of conducting regular cybersecurity health checks of company systems and segregating sensitive data so it isn't all located in one place.

"Hackers shouldn't be able to get 143 million people's information in one swoop," Sharton said.

Companies should also make sure that they have a "very clear governance structure" in place, that they know who's going to take the lead in the event of a breach, and that they've practiced their incident response plans, according to Crowell & Moring LLP partner Evan Wolff.

"Cyber is a team sport," he said. "Threats are constantly changing, and companies need to be prepared."

Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and chair of the firm's privacy and data security group, said the Equifax breach serves to underscore the "sophistication and complexity of this threat," and that companies can never take too many precautions to ensure that the sensitive and valuable data they hold is protected.

"Cybercriminals follow the money, and this hack is no different," he said.

The Georgia plaintiffs are represented by John Yanchunis and Marisa Glassman of Morgan & Morgan Complex Litigation Group, and John R. Bevis, Roy E. Barnes and J. Cameron Tribble of Barnes Law Group LLC. The Oregon plaintiffs are represented by Michael Fuller and Rex Daines of OlsenDaines PC, Justin Baxter of Baxter & Baxter LLP, Robert Le and Kelly Jones.

Counsel information for Equifax was not immediately available.

The cases McGonnigal et al. v. Equifax Inc., case number 1:17-cv-03422, in the U.S. District Court for the

Northern District of Georgia, and McHill et al. v. Equifax Inc., case number 3:17-cv-01405, in the U.S. District Court for the District of Oregon.

--Editing by Pamela Wilkinson and Mark Lebetkin.
