Federal Court Decision Demonstrates Ongoing Challenges Faced by Plaintiffs in Data Breach Litigation

On February 11, 2015, the U.S. District Court for the Southern District of Texas dismissed a class action complaint against the St. Joseph Health System arising out of a data security breach that occurred after hackers allegedly infiltrated the St. Joseph computer network in December 2013. In her complaint, the plaintiff alleged violations of the Fair Credit Reporting Act as well as various state and common law claims sounding in tort and contract. U.S. District Judge Kenneth M. Hoyt granted the defendants' motion to dismiss, holding that the plaintiff failed to allege a cognizable Article III injury and therefore lacked standing to bring her federal claims. The *St. Joseph* decision highlights the emerging majority view in data security breach cases that the mere heightened risk of future misuse of stolen data is too speculative to create standing for the purposes of Article III.

St. Joseph is a Texas-based health care services provider. As alleged in the complaint, patients of St. Joseph, including the plaintiff, provide personal information to St. Joseph in the course of purchasing health care services. This information, according to the complaint, is stored on the St. Joseph computer network and includes names, social security numbers, birthdates, addresses, medical records, and bank account information. On February 4, 2014, St. Joseph announced that hackers had infiltrated its computer network over three days in December 2013 and potentially gained access to the information of 405,000 St. Joseph patients and employees, including the plaintiff. Upon discovery of the attack in December 2013, St. Joseph shut down access to the involved computer. In its letter disclosing the breach, St. Joseph reported that it was not aware that any personal information had thus far actually been misused. Further, St. Joseph made arrangements to provide potentially affected persons with one year of free credit monitoring and identify theft protection and requested that individuals take precautions by monitoring their credit reports and account statements.

The plaintiff's complaint alleged that, after the hackers accessed and stole her information from the St. Joseph network, they disseminated it into the public domain where it was misused by unauthorized and unknown third parties. According to the complaint, various unknown third parties had attempted to charge a purchase to her credit card; attempted to access her Amazon.com account; caused her to receive telephone solicitations from medical products and services companies; sent spam email from her email account; and caused her to receive physical and electronic materials targeting her recorded medical conditions. Further, the plaintiff claimed that, based on information gleaned from the Government Accountability Office and the Federal Trade Commission, she and her fellow class members were now more vulnerable to future attacks by individuals who may seek to commit any number of identity theft-related crimes. Accordingly, the plaintiff alleged willful and negligent violations of the FCRA by St. Joseph in addition to state and common law claims, and sought injunctive relief and statutory damages. According to the complaint, but for St. Joseph's failure to safeguard her personal information and timely notify her of the data security breach, her identity would not have been exposed, stolen and misused, nor would she have suffered "additional economic damages and other actual harm."

St. Joseph moved to dismiss the complaint under Rule 12(b)(1), arguing that the court lacked subject matter jurisdiction to hear the claims because the plaintiff did not suffer any actual or imminent injury that was traceable to St. Joseph's conduct. The plaintiff contended that she had suffered both an actual injury, in the form of the specific instances of fraud, and an imminent injury, in the form of an "increased risk of additional real and impending" theft or fraud.

Foremost, the court held that the plaintiff lacked standing to bring her federal claims to the extent they were premised on the heightened risk of future identity theft or fraud. Relying on the 2013 Supreme Court

case *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), the court found that to establish an imminent injury sufficient to satisfy the requirements of Article III, the plaintiff must at least plausibly establish a "certainly impending" or "substantial" risk that she will be victimized. The court found that the mere "increased risk" of future identity theft or fraud is not a "certainly impending" or "substantial" risk required for standing under Article III. Though the court acknowledged her fear that "savvy thieves" could fraudulently use her personal information at some time in the future, such alleged future injuries remained "speculative" or "hypothetical," but "certainly not imminent." The court noted that, "[c]ritically, [the plaintiff] cannot describe how she will be injured without beginning the explanation with the word 'if.'" However, the mere "allegation that risk has been increased does not transform that assertion into a cognizable injury."

With regard to the plaintiff's claims that an "actual injury" had occurred as a result of the breach, the court found that the allegation that St. Joseph's failures proximately caused these injuries (to the extent they were even actual injuries at all) was conclusory and "fail[ed] to account for the sufficient break in causation caused by opportunistic third parties." In addition, the court found that even if the alleged injuries were traceable to St. Joseph's conduct, the plaintiff failed to allege any quantifiable damage or loss she suffered as a result of the data security breach and most of the alleged injuries had already been remedied. For example, Discover never charged the plaintiff for the fraudulent attempted purchase on her credit card. Finally, the court found that the plaintiff failed to demonstrate the redressability of many of her alleged injuries—a ruling by the court could not prevent third-party companies from contacting the plaintiff with solicitations. As the court's 12(b)(1) ruling regarding plaintiff's standing was dispositive, the court did not reach the viability of the plaintiff's claims under Rule 12(b)(6).

The *St. Joseph* opinion highlights the significant burden imposed by *Clapper* and its progeny on data security breach plaintiffs, which we described in a client alert shortly after *Clapper* was decided. The *St. Joseph* court's analysis made clear that the heightened risk of future identity theft or fraud in the wake of a data security breach is too speculative to confer Article III standing. Indeed, in the wake of *Clapper*, most courts that have considered the issue have reached the same conclusion, while a few other courts have held that a credible threat of identity theft would suffice. The *St. Joseph* court also noted that *Clapper* stands for the proposition that a plaintiff cannot incur costs to avoid an injury that is not certainly impending (such as costs to enroll in credit monitoring) and thereby "manufacture" standing. Further, the *St. Joseph* decision makes clear that even if a plaintiff alleges an actual injury, she will have to establish both causation and redressability to have standing, which will require more than mere conclusory assertions. Going forward, it is likely that standing will continue to be a focus for courts in private data security breach litigation, and will often be dispositive.

For more information regarding the *St. Joseph* decision and its potential impact or to discuss data security practices generally, please feel free to contact a member of Ropes & Gray's leading privacy & data security team or your regular Ropes & Gray contact.