Court Considers Victims' Right to Sue Over Data Breach

by Steve Kramarsky

What do a "smart" TV, a casino fish tank, and a talking teddy bear have in common? They have all been used, over the past year, to steal people's personal information.

It is no secret that large-scale data breaches have become increasingly prevalent in the last several years. In the first half of 2017, there were reportedly "a record 791 data breaches in the United States, up 29 percent from the same period a year earlier." Tiffany Hus, "Data Breach Victims Talk of Initial Terror, Then Vigilance," (Sept. 9, 2017). From Yahoo, which exposed account details, names, and personal information associated with its three billion accounts, to Equifax, which revealed highly sensitive financial information relating to 143 million consumers (Seth Fiegerman, "The biggest data breaches ever," (Sept. 7, 2017)), the scale and scope of these breaches seems to grow larger every day. Concerns about "Nigerian Princes" gaining unauthorized access to our bank accounts now seem quaint.

Perhaps one cost of our increasingly interconnected online existence is increased vulnerability to cyber-criminals, who make a living exploiting vulnerabilities in the firms and devices we trust with our sensitive personal information. Cyber-criminals can use such information to open fraudulent accounts, claim tax refunds, and even set up sham companies in their victims' names. One analysis indicated that, in 2016, more than 15 million Americans were victims of such identity theft, at a cost of some $16 billion. In response to these kinds of threats, many companies have increased cybersecurity spending and developed robust cybersecurity policies. E.g., Helen Reid, "Cyber security stock rise in wake of global 'ransomware' attack," (May 15, 2017). But what happens when those defenses fail, or worse, when companies don't bother with them at all?

Despite the severity of the potential harms in these cases, and the need to protect consumers, private individuals have had mixed success recovering damages from companies who expose their sensitive information to cyber-criminals. As in any case, plaintiffs in these actions must demonstrate that they have standing, as well as a substantive basis for relief. Plaintiffs who know that their sensitive information has been exposed, but who cannot point to any particular example of identity fraud, may find their claims dismissed for lack of a "certainly impending" injury sufficient to afford standing. See Whalen v. Michael Stores, 153 F. Supp. 3d 577, 583 (E.D.N.Y. 2015) (dismissing claim because risk of further harm due to exposure of sensitive information was not a "certainly impending" injury).

Courts in several recent cases have struggled with this issue, recognizing the potential tension between the

constitutional requirements of standing and the increasing need to protect the personal information of individuals. A recent decision from the Southern District of New York examines that balance and the scope of a company's duty to protect the sensitive information of its employees and customers. It is worth a closer look.

'Sackin v. TransPerfect'

In February 2017, employees of TransPerfect Global, a translation services company with over 4,000 employees, filed a class action against their employer alleging damages from a "data breach of TransPerfect's computer systems." Sackin v. Transperfect Global, 2017 WL 4444624 (S.D.N.Y. Oct. 4, 2017). In January 2017, TransPerfect suffered a data breach as a result of a "phishing" scheme. One or more TransPerfect employees had received an email that "appeared to come from TransPerfect's CEO, but actually was sent by unidentified cyber-criminals," in which the sender requested sensitive information, including W-2 forms and payroll information, for all of TransPerfect's thousands of current and former employees. At least one TransPerfect employee complied with the request, presumably believing it came from TransPerfect's CEO, and sent the requested information, in unencrypted format, to the unidentified hackers. "As a result, cyber-criminals obtained Plaintiffs' names, addresses, dates of birth, Social Security numbers," and banking information. Id. at *1.

Importantly, for purposes of this case, the court pointed out that TransPerfect was well aware of "the prevalence of cyber-attacks on corporate records" and the gravity of the risk posed by such attacks. TransPerfect maintained "a corporate privacy policy and security manual that described 'robust procedures designed to protect the PII with which it is entrusted'" and publicly warned clients never to send sensitive information by email because "email 'is generally not secure' and is the method of communication 'most vulnerable to hacking.'" Id. But despite that knowledge, the court held that TransPerfect did not take the basic security precautions that other, similarly situated corporations take. It did not train employees on data security, "erect digital firewalls," or maintain PII retention and destruction protocols.

Plaintiffs thus filed an amended complaint in May 2017 seeking damages arising from the breach for common law negligence, breach of express and implied contracts, unjust enrichment, and violation of N.Y. Labor Law §203-d, which prohibits employers from publicly disclosing the personal information of their employees. TransPerfect moved to dismiss for failure to state a claim and lack of standing, but Judge

Lorna Schofield denied the motion as to all claims except the breach of express contract claim. The opinion turns on the scope of TransPerfect's duty to protect the personally identifiable information, or "PII," in its care.

The First Hurdle: Standing

The court first considered whether plaintiffs had standing to pursue their claims. The primary question here was whether plaintiffs had alleged a sufficiently imminent harm to satisfy the standing requirement of injury-in-fact, given that plaintiffs did not allege their PII had yet been used by cybercriminals for any nefarious purpose. Under Article III of the Constitution, standing cannot be based on speculative future harm; a plaintiff must allege violation of "legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." John v. Whole Foods Mkt. Grp., 858 F.3d 732, 736 (2d Cir. 2017).

The court found that the disclosure of plaintiffs' PII "directly to cyber-criminals creates a risk of identity theft sufficiently acute to fall comfortably into the category of 'certainly impending.'" Central to that conclusion were the kind of information taken and the likely motivation of the phishing scheme: The court held that the only possible purpose of the phishing email was to acquire highly sensitive information (including Social Security numbers and bank accounts) and either use it nefariously or sell it to someone who would. Under those circumstances, plaintiffs could reasonably expect imminent harm. In addition, plaintiffs' decision to spend money on additional monitoring and security services (beyond those offered by the company after the breach) were another source of compensable harm that conferred standing. Sackin, 2017 WL 4444624, at *3.

The court noted that its decision was in line with other circuit courts, which have consistently "held that Article III does not require Plaintiffs to wait for their identities to be stolen before seeking legal recourse." Id. at *2 (citing Attias v. Carefirst, 865 F.3d 620, 629-30 (D.C. Cir. 2017); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 695 (7th Cir. 2015); Galaria v. Nationwide Mut. Ins., 663 Fed. Appx. 384, 388 (6th Cir. 2016); Anderson v. Hannaford Bros Co., 659 F.3d 151, 164 (1st Cir. 2011)). While the Second Circuit has not yet addressed the question of standing in such situations, recent decisions have indicated it is a question of fact to be determined on a case-by-case basis. The court also distinguished contrary decisions in which either the exposure or the amount of information was relatively minimal, from this case, in which the most sensitive information was provided directly to presumed cybercriminals.

Substantive Issues and Rule 12(b)(6)

Next, the court considered whether plaintiffs had adequately pled causes of action for negligence, breach of express and implied contracts, unjust enrichment, and violation of N.Y. Labor Law. The court denied defendants motion to dismiss on all of those claims except the claim for breach of an express contract, which was dismissed because Plaintiffs' employment contracts contained no express agreement by TransPerfect to protect their PII.

In upholding plaintiffs' claim for common law negligence, the court explicitly held that employers have

a duty to take "reasonable precautions" to protect the PII they collect from employees. Sackin, 2017 WL 4444624, at *4. Employees are not well situated to protect such information, as it is in the hands of the company. Absent potential liability, employers may lack the proper economic incentives to take reasonable measures to protect against exposure of the PII entrusted to them. The court thus held that plaintiffs could go forward with their claim that TransPerfect had breached its common-law duty by failing to take reasonable precautions to prevent the wrongful dissemination of their PII, including properly training its employees in data security and deploying appropriate technological protections such as firewalls. The court rejected (at least at this stage) TransPerfect's argument that it had no duty to control the conduct of third parties—whether its employees who responded to the phishing email or the cybercriminals who sent it.

The court also upheld plaintiffs' breach of implied contract claim. It held that TransPerfect had made an "implicit promise" to take reasonable measures to protect its employees' PII when it required and obtained the PII as part of the employment relationship. This implicit promise was also contained in the company's privacy policies and procedures, which it held out as being designed to protect PII. The court held that plaintiffs' claim for unjust enrichment could go forward, because TransPerfect was enriched by plaintiffs' labor and at their expense, due to its decision to "cut costs" by not implementing reasonable security measures to protect the PII.

Finally, the court considered plaintiffs' claim under N.Y. Labor Law §203-d, which imposes strict liability on employers who reveal employees' PII. While the text of that statute does not explicitly create a private right of action, the court held that it was appropriate to permit one under the circumstances: Plaintiffs were amongst the class for whose benefit the statute was enacted, the recognition of a private right of action would promote the legislative purpose, and the creation of such a right would be consistent with the legislative scheme and would not require special agency expertise to implement. Notably, TransPerfect's violation of the statute was also an additional basis for the courts' holding that plaintiffs' negligence claim could go forward, as that violation constituted negligence per se.

Towards a Standard of Care

Personal information is, to a great extent, the currency of the modern Internet. It is nearly impossible to have a life online without giving your sensitive information to someone, and multi-billion dollar businesses are now built on the collection, aggregation, and analysis of that information.

That business model can look pretty good from the consumer side. We get to enjoy "free" services provided by the Googles and Facebooks of the world, but we tend to undervalue our personal information—until it falls into the wrong hands. Yesterday's "free" can all-too-quickly cost us dearly for years to come. There are technological safeguards, but technology is always an arms race and criminals have strong economic incentives to pursue their prize as aggressively as possible. The companies charged with safeguarding the prize don't necessarily have similar market incentives (because individual consumers don't vote with their dollars or don't even have a choice) so the law may have to provide them.

Sackin is an excellent example of a court that understands this big picture and took a measured approach to the problem. Clearly, there must be some duty for companies to protect the data entrusted to them. While the contours of that duty are far from clear, Sackin identifies areas of consensus as to the factors to be considered. The type of data matters (disclosure of extremely sensitive information such as bank account numbers and Social Security numbers is most likely to form the basis for a claim) as does the existence and adequacy of preventative measures. These remain fact-intensive inquiries, but the parameters set out by the Sackin court offer some well-reasoned guidance.

Stephen M. Kramarsky, a member of Dewey Pegno & Kramarsky, focuses on complex commercial and intellectual property litigation. John Millson, an associate at the firm, provided substantial assistance with the preparation of this article.

This article first appeared in the *New York Law Journal* on November 20, 2017.