No good deed goes unpunished: Did P.F. Chang's prompt notice of data breach create standing to sue?

April 18, 2016

Class-wide relief for security breaches just got a little easier in the Seventh Circuit.

On April 14, 2016, the court released its opinion in Lewert v. P.F. Chang's China Bistro, Inc., 2016 U.S. App. Lexis 6766 (7th Cir. 2016), holding that class plaintiffs may satisfy Article III standing by alleging both an increased risk of fraudulent charges and identity theft, as well as costs incurred in mitigating a future risk of harm. Although this is the second time the Seventh Circuit has addressed standing in this context (see Remijas v. Neiman Marcus Group, LC, 794 F.3d 688 (7th Cir. 2015)), the case expands the court's already generous standard. It also illustrates the difficult choices faced by companies whose systems are hacked.

The plaintiffs each ate at the P.F. Chang's restaurant in Northbrook, Illinois, in April 2014 and paid their bills using their debit cards. In June, the company announced that its computer system had been hacked and that some consumer credit and debit card information had been stolen. Of course, the company could not know the scope of the hack at first but immediately warned those who dined at all of its stores of the bad news. It later determined that just 33 locations were affected, and the restaurant where the plaintiffs ate in Northbrook, Illinois, was not among them. It also implemented the use of manual credit card processing at all of its locations to ameliorate any ongoing risk arising from the hack.

Nonetheless, the "damage" was done. One of the plaintiffs discovered four unauthorized transactions on his debit card and, "putting two and two together," concluded that his debit card was among those that had been hacked. Lewert, 2016 U.S. App. LEXIS 6766, at *3. He cancelled his debit card and purchased credit monitoring protection.

The other plaintiff was more fortunate. There was no unauthorized activity on his debit card, so he did not cancel his card, purchase credit protection or suffer any type of cost. But, he claimed that he was injured because he spent time monitoring his credit card statements and his credit report to ensure that there was no unauthorized activity. The district court dismissed the complaint, concluding that the plaintiffs had not suffered the requisite personal injury to satisfy Article III standing.

Ordinarily this fact pattern would not be enough to create standing. The general rule is that a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Clapper v. Amnesty Internat'l USA, 133 S. Ct. 1138, 1151 (2013). Nor may standing be based solely on the risk of a future harm. The Supreme Court has "repeatedly reiterated that 'threatened injury must be certainly impending to constitute injury in fact,' and that '[a]llegations of possible future injury' are not sufficient." Id. at 1147. (Emphasis in original) (citations omitted).

Nevertheless, the Seventh Circuit found that the plaintiffs' allegations were sufficient to meet the standing requirement. It found that mitigation costs incurred in purchasing credit protection as well as the risk of future fraud or identity theft were enough to confer standing. Id. at **8-9.

It also rejected P.F. Chang's argument that the plaintiffs lacked standing because their data was not exposed to the breach. Lewert, 2016 U.S. App. LEXIS at **9-10. The court relied on P.F. Chang's initial notice to the public, which suggested that the breach affected customers at all locations:

> When the data system for an entire corporation with locations across the country experiences a data breach and the corporation reacts as if that breach could affect all of its locations, it is certainly plausible that all of its locations were in fact affected. Id. at *11.

There are several aspects of this decision that are troubling. First, permitting mitigation costs and the risk of future harm to confer standing is hard to square with Clapper, which rejected these very arguments.

More disturbing is the court's reliance on P.F. Chang's first public statement about the breach to confer standing. The court said that whether the breach affected the Northbrook, Illinois, location is "a disputed fact" and "a theory of defense that P.F. Chang's will be entitled to pursue at the merits phase," which was enough to reverse the district court's dismissal of the case. Id. at *13.

Setting aside that the burden of proof at the standing phase of a case falls on the plaintiffs and not the defendant (see Clapper, 133 S. Ct. at 1149, n. 4):

- Would the case have come out differently if P.F. Chang's had waited to make its initial announcement until after it learned that only 33 locations were affected?
- Could a plaintiff "plausibly" allege exposure to the data breach if the first public announcement limited the scope of the breach to exclude that claim?
- And what lessons will the victims of cyber attacks draw from this case?

Indeed, the Lewert case will cause some to re-think the prudence of making any announcement of a potential hack until more is known about the nature and scope of the breach.

It will also cause some to re-evaluate mitigating responses to a breach. By focusing on P.F. Chang's decision to "switch to manual card-processing" at all of its locations, the court permitted the plaintiffs to use P.F. Chang's prompt response to the hack as an argument in support of their standing to sue.

Many challenges await the plaintiffs:

- How will any be able to prove that unauthorized use of their debit card was because of this hack, rather than some other?
- How can difficult issues of individual causation ever be decided on a class-wide basis?
- And how can you ever ascertain class membership without deciding the individual claims?

P.F. Chang's may forever wonder if its good deed was worth it.

Authors

Drew H. Campbell

Partner

Columbus
614.227.2319
dcampbell@bricker.com