The Customer is Always Right? Restaurant Patrons Don't Need to Wait Until Hackers Attack

Amundsen Davis Data Security & Breach Legal Update
May 16, 2016

In what could be seen as expanding the opportunities for consumers to pursue data breach cases, the Seventh Circuit recently found that simply taking steps to protect one's finances or credit ratings is sufficient for a federal lawsuit to proceed.

Faced with claims that P.F. Chang's compromised the credit and debit card information of its customers, the appellate court found that consumers could pursue their claims - even without suffering a "hack" - because they had taken action to protect their credit ratings. *Lewert v. P.F. Chang's China Bistro, Inc.,* 2016 WL 1459226 (7th Cir. 2016). The court explained that consumers "should not have to wait until hackers commit identity theft or credit-card fraud" in instances where there "is an objectively reasonable likelihood that such injury will occur."

Sometime in 2013 or early 2014 (P.F. Chang's is not sure when), hackers purportedly stole the credit and debit card numbers of some customers of the restaurant chain. Two customers subsequently brought suit. They complained that after dining at the restaurant, they were informed - by a press release - of the data theft and were then forced to take steps to protect their private information. Those steps included spending time and money monitoring their credit card statements and other financial information for fraudulent charges or identity theft.

On appeal, P.F. Chang's argued that the customers had no right to pursue their lawsuit because the specific restaurant at which the two plaintiffs dined had not been affected by any data breach. Perhaps, in other instances, this argument would carry weight. But, the Seventh Circuit rejected the argument, citing two missteps by the national chain in the wake of the breach.

First, P.F. Chang's was apparently unaware that hackers had compromised customer credit card data until months after the initial breach. It then took the chain even longer to discover the scope of the hack. Next, even before it had a handle on the extent of the intrusion, it sent communications to all customers with incomplete (and incorrect) information concerning the breadth of the breach. For instance, the chain announced that the breach affected all

PROFESSIONALS

John Ochoa
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

AMUNDSEN DAVIS

restaurants but later found only 33 restaurants were compromised. The Seventh Circuit found that, due to this ham-handed response to the breach, it was reasonable to believe (and for the plaintiffs to allege) that all customers' credit card information was stolen. Plaintiffs had sufficiently claimed harm from the breach and the lapses thereafter.

Although this case may not have widespread impact, it brings with it an important lesson: your response to a data breach is just as important as preventing one in the first place. Here are a few things to keep in mind to help your company try to avoid significant missteps in the wake of a data breach:

- Have systems in place to actively monitor for data breaches so that your company can learn of them as soon as possible. You can read more about how to guard against, and react to, a data breach in our data breach starter kit found here;
- Ensure that you have a data protection response team in place to react to data breaches and to collect pertinent information as quickly as possible;
- Have written policies and protocols to ensure that your company's response to a data breach is done in a coordinated and timely manner; and,
- Make sure that the message sent out to your customers concerning the data breach is accurate, timely, and properly vetted.

The Customer is Always Right? Restaurant Patrons Don't Need to Wait Until Hackers Attack