Scottrade wins dismissal of data breach suit (E.D.Mo.)

(July 21, 2016) - Hackers may have illegally accessed Scottrade Inc.'s customers' personal information, but the proposed class members never alleged any actual harm or identity theft occurred in the two years since the breach happened, a Missouri federal judge has ruled.

Duqum et al. v. Scottrade Inc., No. 15-cv-1537, 2016 WL 3683001 (E.D. Mo. July 12, 2016).

Scottrade argued that Andrew Duqum and the other plaintiffs had no constitutional standing to pursue their breach-of-contract, negligence and consumer protection lawsuit against the brokerage firm, and U.S. Magistrate Judge Shirley Padmore Mensah of the Eastern District of Missouri agreed.

Article III of the U.S. Constitution requires plaintiffs to show they have a concrete, particularized, and actual or imminent injury to have standing in federal court.

With no instances of identity theft and no credible allegations that their personal information lost value, Duqum and the others could not show they met the injury-in-fact requirement to establish Article III standing.

Tucker Ellis LLP attorney Paul L. Janowicz, who handles complex litigation including privacy and data security issues at the firm, says the standing issue has been difficult for the courts.

Judges understand the frustration people feel when their information is exposed, but the court system is reserved for people who have suffered an actual harm, he explained.

"While there are certainly exceptions, courts are generally reluctant to find standing when there is no evidence that anyone has used a plaintiff's personal information improperly by, for example, making fraudulent purchases, opening up new credit cards, etc.," he said.

Janowicz was not involved in this case.

Carlton Fields shareholder Kristin Ann Shepard, who handles high-stakes litigation matters and writes and speaks on data-breach class actions and cybersecurity, mentioned how court precedent dictates that standing should not turn on speculation about the decisions of independent actors.

This is good policy, she said, noting how state and federal regulators are in a better position than courts to set industry best practices regarding cybersecurity.

"Businesses already have significant incentives to guard against cyberattacks — including but not limited to the reputational damage, diminished value/share price, cost of customer notification and credit monitoring, and increased cyberinsurance premiums that may follow large-scale breaches," Shepard explained.

"It's also hard to quantify the alleged harm to consumers like those in the Scottrade, Target and Home Depot cases — who received free credit monitoring services after a breach and whose credit card companies reimbursed any fraudulent changes," she added.

Shepard, who works out of the firm's Washington office, also was not involved with the case.

Scottrade's privacy promises

St. Louis-based Scottrade offers brokerage, banking and retirement planning services to individuals and businesses, according to Judge Mensah's order.

Before opening an account, all customers must provide Scottrade with personally identifying information, or PII, such as their names, Social Security numbers, work history and addresses, the order said.

They must also sign a brokerage agreement with the firm, which incorporates the company's privacy policy, according to the order.

The privacy policy states that Scottrade protects and safeguards customers' information using security measures that comply with federal law, the order said.

Additionally, Scottrade's website indicates that the firm securely protects customers' PII, the order said.

Data breach allegedly affects 4.6 million

In August 2015 the FBI alerted Scottrade that hackers had accessed the brokerage firm's systems, stealing customers' PII without its knowledge, Judge Mensah's order said.

Between September 2013 and February 2014, the unauthorized access allegedly allowed hackers to export confidential information for about 4.6 million Scottrade customers.

The hackers used the PII to create a competing database for marketing and brokering stock transactions and to operate a "pump and dump" scheme that amassed millions of dollars, the order said.

According to a Nov. 14, 2015, Reuters article, similar hacks occurred at JPMorgan and ETrade, Fidelity Investments, TD Ameritrade Holding Corp. and News Corp.'s Dow Jones unit.

Prosecutors charged two Israelis and one American fugitive with orchestrating the scheme, the article said.

The co-conspirators would buy penny stocks and spread false and misleading information to boost the prices, promoting them to customers of the hacked financial firm, the article said. Then they would sell the penny stocks at a higher price to make a windfall.

No actual identity theft, fraud alleged

About two months after the FBI notified the brokerage firm of the breach, Scottrade started notifying customers about the breach and offering them one year of credit monitoring and identity theft insurance, according to the order.

Customers began to file lawsuits, which were consolidated in the Missouri federal trial court.

After the customers filed their consolidated class complaint Feb. 19, Scottrade moved to dismiss the suit for lack of standing, arguing the customers failed to allege any injuries-in-fact.

Judge Mensah agreed.

The plaintiffs never alleged any instances of actual identity theft, only an increased risk, but this was too hypothetical, especially because it depended on the actions of third parties — the hackers or criminals, the judge said.

Similarly, the cost of mitigating any hypothetical harm was too speculative to constitute an injury-in-fact, Judge Mensah added.

The customers argued they had a bargained-for expectation that Scottrade would safeguard their personal information, and they failed to receive the full value of the services they bought, which included adequate data security measures.

Judge Mensah rejected this argument, saying it was unclear what portion of the brokerage fees the parties agreed would be allocated toward data security and what value they lost.

She also rejected the customers' claims that they lost value in their personal information.

The customers never alleged they intended to sell their information, they were unable to sell it after the data breach or they needed to accept a lower price because of the breach, the judge said.

Kirkland & Ellis partner Patrick F. Philbin said, "The decision is significant for strengthening the hand of data breach defendants seeking to dismiss claims for lack of standing."

Philbin, who handles data security and privacy litigation, was not involved with the case.

"By holding that evidence of illegal activity is not enough to show an imminent threat of harm to plaintiffs under *Clapper v. Amnesty International U.S.A.*, 133 S. Ct. 1138 (2013), unless the type of illegal activity suggests a direct impact on plaintiffs, the court set a fairly high threshold for establishing standing that defendants will certainly embrace," he said.

Philbin also indicated the decision will almost certainly be appealed to the 8th U.S. Circuit Court of Appeals.

"But the 8th Circuit appears set to address many of the threshold standing issues in data breach cases before *Duqum* is briefed, so *Duqum* might not end up being the test case at the 8th Circuit level," he added, referencing an appeal in *Alleruzzo et al. v. SuperValu Inc. et al.*, Nos. 16-2378, 16-2528, *appellate brief filed* (8th Cir. July 13, 2016).

By Melissa J. Sachs

End of Document