Financial Institutions are Foreseeable Victims in Target Data Breach Cases

Jan 16, 2015

Categories:

Blockchain and Digital Assets
Blogs
Publications

Authors:

Jennifer A. Rulon

In an important decision regarding financial institution claims for recovery of losses resulting from data breaches, the United States District Court in Minnesota recently issued an Order denying Target's attempt to dismiss all claims brought against it by financial institutions.

In December 2013, Target Corporation announced that computer hackers stole credit and debit card information for approximately 110 million of Target's customers over a period of three weeks. Card issuing banks brought claims against Target, alleging Target (1) was negligent in failing to have sufficient security in place to prevent hacking of customer data; (2) negligently misrepresented by failing to advise the card-issuing banks of the insufficient security measures; and (3) violated and was negligent per se for violating Minnesota's Plastic Security Card Act (the "Act"). Under the Act, any person or entity conducting business in Minnesota is prohibited from storing security codes, PIN numbers, or the full contents of any track of magnetic strip data from customers' debit or credit cards for more than 48 hours after authorization of a transaction. Minn. Stat. § 325E.64.

Target moved to dismiss these negligence claims, arguing that it had no duty and did not breach any duty to the banks because there was no special relationship between the parties and the harm, if any, was an unforeseeable result of the hacker's conduct.

The court found that the banks sufficiently alleged that the harm to the card-issuing banks was a foreseeable consequence, whether premised upon the hacker's conduct or Target's alleged disabling of a security feature and failing to react to warning signs in its system. On the banks' claims of negligent misrepresentation by omission, however, the court granted Target's motion to dismiss because the banks failed to specifically plead reliance.

In response to the banks' statutory claim that Target violated the Act and was negligent in doing so, Target first argued that the Act only applies to Minnesota transactions. The court disagreed, stating

that the Act applies to Minnesota companies' data retention practices for both in-state and out-of-state transactions. The court further maintained that the Act does not violate the dormant Commerce Clause because it does not discriminate between in-state and out-of-state transactions. Rather, the Act applies only to Minnesota companies' data security practices and does not attempt to regulate any company not conducting business in Minnesota.

Target also argued that the Act only prohibits the retention of customer data, and because the customer data was stolen when the customer's card was used at a Target store and not from Target's database storage system, Target's alleged retention of that data did not cause harm to the card-issuing banks. The banks responded that (1) Target retained the data because the hackers' malware stored the stolen data on Target's own servers for up to six days before transmitting the data to the hackers, and (2) the hackers would have been unable to steal all of the card's magnetic strip information, including the card's CVV code, without accessing the customer data stored by Target on its servers.

The court did not resolve this factual dispute between the parties regarding the retention of the data—that dispute will be determined if the case is adjudicated on the merits. Instead, the court denied Target's motion to dismiss because the banks sufficiently pled a plausible claim that the hackers retrieved some of the credit and debit card data from Target's servers. Thus, the court upheld the card-issuing banks' claims for negligence and violation of the Act and allowed the claims to proceed on their merits.

This case provides an important basis for financial institutions to plead they are foreseeable victims of data breaches under a theory of negligence. The Plastic Security Card Act is a unique state law, however, that cannot be a basis for liability outside Minnesota.

If you would like additional information about this case, please contact Jennifer Rulon, with Frost Brown Todd LLC, at jrulon@fbtlaw.com or (317) 237-3978.

FBT Gibbons