New Jersey Law Journal

VOL. 208 - NO 6 MAY 7, 2012 ESTABLISHED 1878

COMMENTARY

Negligence Should Be a Viable Cause Of Action for Identity Theft

BY GRAYSON BARBER

In the bad old days, if someone stole your identity, the burden was entirely on you to rehabilitate your reputation. Identity theft victims spent countless hours defending themselves against demands for payment, and some of them spent time in jail.

Fortunately, in 2006, New Jersey enacted its Identity Theft Prevention Act, which provides, among other things, breach notification and data security requirements.

In this day and age, financial institutions know they have a duty to provide reasonable security for personally identifiable information as well as information that can be linked to specific individuals.

This duty is codified in federal law. The first paragraph of the federal Financial Services Modernization Act, better known as Gramm Leach Bliley (GLBA), states that financial institutions have a duty to protect personally identifiable information.

"It is the policy of Congress that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of its customers' nonpublic personal information," it states.

The existence of this duty suggests that negligence should be a viable cause of action against financial institutions that fail to protect personally identifiable information. Corporations already know they should implement security to protect against data theft, adopt reasonable data retention and disposal policies, delete data they no longer need and give customers a chance to correct inaccurate information about themselves.

Gramm Leach Bliley provides no private cause of action, but its plain language states that financial institutions have a legal duty, and that to violate it would constitute a violation of other personal rights.

In a Georgia case, *Jenkins v. Wachovia*, the plaintiff established a negligence claim based on allegations that a bank violated the duty articulated in Gramm Leach Bliley. Marching through the elements, the Georgia Court of Appeals held on Feb. 12 that the plaintiff established the existence of a duty by pleading that the bank falsely represented to customers and the general public that it created and implemented a system to adequately protect private and personally identifiable information entrusted to it.

Alleging a breach of that duty, the plaintiff said that a bank teller who had no need for the information was nevertheless given access to it. The complaint stated that the teller gave the information to her husband, who used the information to steal the plaintiff's identity. This damaged the plaintiff's credit and caused additional injury.

On the bank's motion for summary judgment, the court had to accept as true the plaintiff's allegations that the bank teller did not need the information, and that the bank failed to implement and follow its own security procedures. Also enumerated in the complaint were the bank's alleged failures to detect, report and stop the bank teller's suspicious activities.

Causation is of course an important element of negligence. Ordinarily, the intervening act of a criminal third party is treated as the proximal cause of an injury, but in *Jenkins*, the court found that the actions of the bank teller and her husband were not an unforeseeable consequence. "We cannot conclude that as a matter of law the intervening criminal act in this case — the wrongful appropriation and use of Jenkins's information by an identity thief — was an unforeseeable consequence of the bank's alleged breach of its duty to protect that information."

The appellate court continued, "Although the GLBA does not create a private right of action for a violation of its terms, its plain language states that financial institutions have a duty to protect certain information of their customers."

Strangely, it is still common practice for companies to put the burden on customers to protect their own privacy. Privacy policies are often impenetrable. Particularly turgid are the privacy notices from financial institutions, required by GLBA, but hardly designed to help consumers.

According to research from Carnegie Mellon University, to read all the privacy policies one encounters online in a year would take 76 work days. Gramm Leach

Barber, a solo in Princeton, concentrates on privacy issues.

Bliley, which defines privacy as notice plus a chance to opt out, inspires financial institutions to create privacy notices that are hard to read and look like junk mail.

The security expert Bruce Schneier maintains that personally identifiable information is like hazardous waste. "Data is the pollution of the information age. It is a natural by-product of every computer-mediated interaction. It stays around forever, unless it's disposed of. It is valuable when reused, but it must be done carefully. Otherwise, its after-effects are toxic," he says.

The metaphor is apt. Significant responsibilities attach to collection of personal data. Consumers can and should push back against the current trend, which is to make privacy protection an individual burden. Financial institutions collect, process and disclose personal financial information. They, like other corporations, must bear their share of responsibility for protecting against identity theft. ■