TRAUB LIEBERMAN

CYBER LAW BLOG

May 30, 2019

Virginia District Court Finds No Common Law Duty to Safeguard Confidential Information on Behalf of Third Party In Wake of Data Breach

BY: Jason Taylor

Plenty has been written about businesses' potential liability to consumers or those harmed directly from a data breach. Less publicized, however, are instances where third party thieves use information obtained in a data breach or business email compromise scheme to obtain money or information from yet another source.

The question arises of whether and/or how to impose liability on a party whose potentially negligent conduct resulting in a data breach causes damages to third parties whose data was not stolen or compromised in the breach. Recently, the Eastern District of Virginia addressed and added its analysis to this developing area of law in Deutsche Bank Nat'l Tr. Co. as Tr. for Home Equity Mortg. Loan Asset-Backed Tr. Series Inabs 2006-A v. Buck, 2019 WL 1440280 (E.D. Va. Mar. 29, 2019), finding that the claimants had failed to establish that Virginia law recognizes a common law duty to protect an individual's private information from an electronic data breach. As such, the Court dismissed their claims, albeit with leave to amend.

The allegations in Deutsche Bank arose from a real estate transaction in which an unidentified, non-party hacker allegedly caused funds to be misdirected to the hacker and away from the proper party, Deutsche Bank. Deutsche Bank engaged the Buck law firm to perform the closing as part of the real estate transaction. Deutsche Bank had also engaged Altisource to act on its behalf in effectuating the transaction, including communicating with the parties and facilitating the sale and closing. As part of its duties, Altisource communicated with the Buck Parties and were to convey payoff instructions for the closing.

According to the Buck Parties, prior to closing a hacker obtained access to Altisource's confidential email communications containing financial information of Altisource's customers, including Deutsche Bank. From this breach, the hacker apparently learned of the upcoming funds transfer between the buyer of real estate and Deutsche Bank, and provided fraudulent wiring instructions to the Buck Parties using a "mimicked" email address to appear as if the instructions came from Altisource.

The Buck Parties received the transfer money from the buyer and, following the fraudulent wiring instructions, wired the money to a bank account presumably belonging to the hacker. Deutsche Bank never received the funds and it sued the Buck Parties for the loss. The Buck Parties, in turn, brought in Altisource as a third-party defendant alleging that it "knew or should have known of the hacking that had been taking place in its email…and…failed to notify and warn its customers (like Deutsche) or those with whom it had business (like the [Buck Parties])."

The third-party complaint against Altisource alleged two theories of liability: contribution and equitable indemnification. Notably, the Buck Parties did not raise any claim or duty stemming from a statute or regulation. Rather, the Buck Parties alleged that Altisource had breached duties it owed to Deutsche Bank (not the Buck Parties), including, generally, a duty to use reasonable care to secure confidential and financial information stored on its systems. The third party complaint alleged that Altisource's acts constituted the proximate cause of the loss, not the Buck Parties' failures in identifying the fraudulent instructions and transferring the money to the hacker's account. Altisource moved to dismiss the third party complaint on the basis that it owed no common law "duty" to the Buck Parties to safeguard the private information of a third party.

As the Deutsche Bank court noted, case law directly on point is sparse. Some courts have found that a party may proceed on a negligence claim against an entity that suffered a data breach. For example, in In re Target Corp. Customer Data Security Breach Litigation, 64 F. Supp. 3d 1304 (D. Minn. 2014) a Minnesota District Court, at the motion to dismiss stage, found that the plaintiffs "plausibly pled a general negligence case," where they alleged that Target "disable[ed] certain security features and fail[ed] to heed the warning signs as the hackers' attack began." Id. at 1309-10.

Other courts, however, have been reluctant to recognize such claims based on a negligence theory of failing to reasonably secure confidential information prior to a data breach. In one example, an Illinois District Court in Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 2017 WL 1551330 (S.D. Ill. May 1, 2017) dismissed plaintiffs' negligence claims against Schnuck after Schnuck was the target of a data breach compromising unencrypted credit card data of its customers. In that case, Plaintiffs (a group of financial institutions claiming to be third party beneficiaries of contracts between Schnuck and its credit card processing companies) claimed that Schnuck's negligence in securing its unencrypted customer credit card data caused them to suffer loss from subsequent fraudulent transactions using the data.

The Schnuck court, applying Missouri law, held Schnuck had no duty to protect customer information on the Plaintiffs' behalf, and therefore, dismissed the negligence claims. Id. at *2-4; see also Landale Signs & Neon, Ltd. v. Runnion Equip. Co., 2016 WL 7409916 (N.D. Ill. Dec. 22, 2016) (finding that where the purchaser presumably sent the payment to a hacker because of a fraudulent email, no duty existed to support the seller's negligence claim because the Illinois Supreme Court had not declared that a duty to safeguard another's confidential information existed, meaning that the legislature, and not a lower court, should act); Willingham v. Global Payments, Inc., No., 2013 WL 440702 (recommending that the district court dismiss plaintiffs'negligence claims because under Georgia law "no duty of care exists in the data breach context where … there is no direct relationship between the plaintiff and the defendant").

Ultimately, the Deutsche Bank court found that the Buck Parties had failed to establish that Virginia law recognized a common law duty to protect an individual's private information from an electronic data breach. Consequently, the Buck Parties could not establish that Altisource owed a common law duty to Deutsche Bank, a necessary element to support a showing of negligence, and in turn, the equitable indemnification and contribution claims against Altisource. The District Court granted Altisource's motion to dismiss the third party claims, but granted leave for the Buck Parties to amend their claims against Altisource.

It is important to note that the claims addressed in Deutsche Bank were based on common law liability theories of equitable indemnification and contribution, which were in the end grounded in negligence, and not statute or regulation (or even privity of contract). Thus, the District Court did not address whether such claims might be viable under Virginia's Breach Notification Statute, Consumer Protection Act, or some similar federal law or regulation pertaining to Altisource's data security obligations. Ultimately, whether or how to impose liability on a party whose potential negligence to third parties flows from a data breach may depend on the particular state's breach notification laws or other data security framework, which may permit a direct cause of action against those that fail to adequately store or handle protected information. If Deutsche Bank is any indication, a third party's reliance solely upon common law duties to protect confidential data of a third party to establish liability in the wake of a data breach may not suffice.