Chicago Daily Law Bulletin®

Volume 163, No. 149 Serving Chicago's legal community for 162 years

Online purchasing platform runs afoul of data breach laws, gets reprimand

E-commerce company Aptos Inc is facing legal action on two fronts as a result of not only its alleged failure to comply with state data security and breach notification laws, but also for giving bad advice about those laws to its clients in the wake of a data breach that compromised personal information of some of its clients' online retail customers.

The attorneys general of Illinois and 14 other states have put Aptos Inc. on notice that they believe that the company is giving its retail clients incorrect information about the consumer notification obligations in those states, following a data breach last year.

At the same time, a proposed class action accuses Aptos of failing to protect customers' personal information, including credit and debit card data, to disclose the extent of the breach and to timely notify affected clients.

Both actions stem from Aptos' discovery last year that hackers installed malware on its servers, exposing 40 of its clients, including Tempur Sealy International Inc. and Liberty Hardware Manufacturing Corp., to possible identity theft.

In a June 5 letter, the attorneys generals of Illinois, Arkansas, Colorado, Connecticut, Iowa, Kentucky, Maryland, Minnesota, Mississippi, New York, North Carolina, Oregon, Pennsylvania, Virginia and Washington notified the Atlanta-based Aptos' general counsel that the company gave clients incorrect information concerning the states' data breach notification laws.

According to the letter, Aptos told the 40 online retailers affected by a data security breach it reported on March 1 that the retailers did not have to notify consumers of the breach in cases where a credit or debit card's CVV number — the three- or four-digit security number — was not compromised.

A frequently asked questions document that Aptos gave clients specifically addressed the question: "What is the notification obligation where CVV data was not exposed?" The FAQ stated in response that there was no obligation to notify consumers if their card's CVV number was not exposed.

"This is not correct. The CVV number does not have to be disclosed to trigger our states' notification obligations," the letter pointed out. All 15 states have similar statutes that mandate notice when personal information plus an "account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account" is acquired by an unauthorized third party, the letter said.

But a CVV number is not considered "any required security code" under the statutory language because a credit card owner — and therefore an identity thief as well — can use a credit card without it, said the letter. In fact, some top websites don't require a CVV code to make a purchase, such as Amazon.com, Freshdirect.com, Zappos.com, Victoriasecret.com and HSN.com, it noted.

The letter, sent by the office of New York Attorney General Eric T. Schneiderman on behalf of the states, noted that New York's statute, for example, is designed to notify affected consumers in the event of a breach so that they can protect themselves from identity theft.

So if a credit card can be used without a CVV number, then the owner of the card should be notified of a breach so he or she can protect themselves. "Any other reading would eviscerate the clear intent of the statute," the letter concluded.

Finally, the state attorneys general informed Aptos that they expect the company to take action and give affected clients the correct data breach information regarding CVV numbers.

On June 9, New York resident Michelle Provost filed a proposed class-action lawsuit against Aptos and its client Tempur Sealy in a federal court in Georgia. The complaint alleges Aptos as well as Tempur Sealy failed to notify customers about the data breach.

Provost used her debit card to make two online purchases from Tempur Sealy in April and June 2016, but didn't find out that her card's information was compromised until April 2017, when Tempur Sealy notified her in writing, according to the complaint. Upon reviewing her bank statements, Provost discovered a fraudulent charge.

The complaint alleges the defendants' deceptive trade practices violate state consumer protection and data breach notification laws and accuses the defendants of negligence, breach of implied contract and unjust enrichment.

It proposes the certification of state and nationwide classes of consumers and seeks actual and statutory damages, restitution and disgorgement. The complaint also asks for an injunction ordering the defendants to promptly notify all affected customers of future data breaches.

According to the complaint, Aptos and Tempur Sealy's actions were a compendium of what not to do with respect to notifying consumers in the event of a data breach. Aptos discovered the data breach in November 2016 and reported it to federal law enforcement agencies. At the agencies' request, Aptos delayed informing clients, including Tempur Sealy, to allow the investigation to move forward, the complaint notes. Aptos notified its clients in February 2017 but took no steps to inform consumers of the breach.

"Instead, Aptos let the online businesses affected decide if, how and when to notify their customers," the complaint states. Tempur Sealy, in turn, didn't tell customers about the breach for nearly another two months, it adds.

Further, neither Aptos nor Tempur Sealy disclosed the extent of the data breach including,

"Instead, Aptos let the online businesses affected decide if, how and when to notify their customers," the complaint states.

PRIVACY, TECHNOLOGY AND LAW

NERISSA COYLE MCGINN

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

how many consumers' personal information — including name, address, e-mail address, telephone number, payment card account number and expiration date — was stolen and when the records were compromised, according to the complaint.

By failing to give adequate notice of the data breach, both defendants prevented consumers around the country from taking steps to protect themselves. Provost said she never would have used her debit card at Tempur Sealy's online store if she had known about the breach.

Finally the complaint alleges the defendants also failed to comply with industry standards to protect customers' personal information. Members of the payment card industry, or PCI, established a Security Standards Council in 2006 to develop PCI Data Security Standards (PCI DSS) to improve the security of payment processing systems.

Aptos and Tempur Sealy failed to comply with the PCI DSS, which requires merchants and service providers to, among other things, protect cardholder data, maintain a vulnerability management program, implement strong access control measures and regularly monitor and test networks, the complaint avers.

With countless data breaches occurring at organizations around the country over the past several years, the Federal Trade Commission issued "Data Breach Response: A Guide for Business" at the end of 2016. The guidance provides details on how to secure the organization's systems, fix the breach — and notify the parties involved, including consumers.

The FTC recommends the organization designate a point person in the organization to release information to those affected by the breach. The agency offers sample letters, websites and toll-free numbers to communicate with people whose information may have been compromised.

The FTC also recommends being as transparent as possible by clearly communicating what is known about the breach, including how it happened, what information was taken, how the stolen information was used if known, what actions are being taken to remedy the situation and how to reach the relevant contacts in the organization.

In addition, the organization should encourage individuals who discover that their information has been misused to file a complaint with the FTC via IdentityTheft.gov.

Most states have enacted legislation requiring notification of security breaches involving personal information, but some are more comprehensive than others.

Illinois amended its Personal Information Protection Act, effective Jan. 1, to require state government agencies and businesses subject to the federal Health Insurance Portability and Accountability Act (HIPAA) that experience a data security breach to notify the state attorney general's office and any affected Illinois residents.

The state attorney general's office also created a dedicated e-mail address for breach reporting: databreach@atg.state.il.us.

Under the Illinois Personal Information Protection Act, any entity that conducts business in the state, and for any purpose, handles, collects, disseminates or otherwise deals with nonpublic personal information, is required to timely disclose a data security breach of personal information concerning Illinois residents.

Organizations subject to HIPAA must provide the state attorney general's office with similar information about the breach and provide additional information including the date and types of any consumer data security breach notification that has or will be sent to consumers and the types of consumer credit monitoring and fraud prevention and detection services being offered, if any.

As Aptos is learning the hard way, regulatory enforcement and consumer class actions are a hefty consequence for failing to conscientiously comply with state data security and breach notification laws