

Letter from the Office of the New
York State Attorney General to
Aptos, Inc. regarding Aptos
communications with client-
retailers resulting from data
breach





STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE
BUREAU OF INTERNET
AND TECHNOLOGY

June 5, 2017

VIA EXPRESS MAIL

David Baum, Esq.
General Counsel
Aptos, Inc.
945 East Paces Ferry Road, Suite 2500
Atlanta, Georgia 30326

RE: Aptos Communications with Client-Retailers Resulting from Data Breach

Mr. Baum:

I am writing on behalf of the Offices of the Attorneys General of New York, Connecticut, Colorado, Pennsylvania, Virginia, Mississippi, Illinois, North Carolina, Kentucky, Oregon, Iowa, Arkansas, Washington, Maryland and Minnesota to address a description of our state data breach notification laws provided by Aptos, Inc. to forty (40) online client-retailers affected by Aptos' recent data security breach reported March 1, 2017 (the "Breach").¹

In particular, we have learned that Aptos, in a "FAQ" provided to its client-retailers, indicated that the retailers do not have to provide consumer notification of the Breach in cases where a credit card CVV number was not disclosed. Specifically, the FAQ provided:

What is the notification obligation where CVV data was not exposed?

As noted in the earlier FAQ, we have received questions about notification obligations in those states whose laws require disclosure only if a financial account number and security code were both exposed. As you know, Aptos is not able to offer legal advice to the retailers. To be clear, Aptos' own view is that there is no obligation to notify in those states - the "account number plus CVV" states - if your customers' CVV data was not exposed. We understand those states to be Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Iowa, Idaho, Illinois, Indiana, Kentucky, Louisiana, Maryland, Michigan, Minnesota, Missouri, Mississippi, Montana, North Dakota,

¹ States not a signatory to this letter should not be construed as approval of Aptos' interpretation of that state's data breach notification law.

Nebraska, New Hampshire, New Jersey, Nevada, New York, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming. We understand that in these states, some retailers with no exposure of CVV codes may choose in an abundance of caution to make voluntary disclosure to consumers and AGs. That is a business judgment for each retailer to make.

This is not correct. The CVV number does not have to be disclosed to trigger our states' notification obligations.

By way of example, New York General Business Law § 899-aa(1)(b)(3) provides for 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 other state signatories to this letter have laws with virtually identical language.² A CVV code is not "any required security code" because a credit card owner, and thus an identity thief, can use a credit card without it. Indeed, some of the most popular websites do not require a CVV code to make a purchase, including Amazon.com, Freshdirect.com, Zappos.com, Victoriasecret.com and HSN.com. The legislative history in New York makes clear that the statute is designed to notify affected consumers in case of a breach so they can protect themselves from identity theft. *See* GBL § 899-aa, Laws 2005, ch 442, §§ 1 eff Dec 7, 2005 ("Therefore, the legislature enacts the information security breach and notification act which will guarantee state residents the right to know what information was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage that has or may occur as a result of the breach.") If a consumer's credit card can be used without a CVV number, then they should receive notice so they can protect themselves. Any other reading would eviscerate the clear intent of the statute.

We expect Aptos to acknowledge receipt of this letter and the presented interpretation of our state data breach notification laws provided herein, and to take actions consistent with this clarification, including without limitation, notifying all of its affected client retailers of this clarification.

Sincerely,



Clark Russell
Deputy Bureau Chief

² *See* Breach of Security re Computerized Data Containing Personal Information, Conn. Gen. Stat. § 36a-701b; Colorado Notification of Security Breach § 6-1-716; Pennsylvania's Breach of Personal Information Notification Act, 73 P.S. §§ 2301; Virginia Code § 18.2-186.6; Mississippi Notice of Breach of Security, Miss. Code Ann. § 75-24-29; Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.*; Ky. Rev. Stat. 365.732; North Carolina Identity Theft Protection Act, N.C. Gen. Stat. § 75-65; Oregon Consumer Identity Theft Protection Act, ORS 646A.600; Iowa Personal Information Security Breach Protection Act, Iowa Code § 715C; Arkansas Disclosure of Security Breaches, Ark. Code Ann. § 4-110-105; Washington Data Breach Notification Law, RCW 19.255.010; Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3501 (2013 Repl. Vol and 2016 Supp.); Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61.