BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

September 12, 2018

Honorable Gary Gensler, Chair
Financial Consumer Protection Commission
3E Senate Office Building
Annapolis, MD 21401

Re: Consumer Protection Division's Overview of Data Breaches

Dear Mr. Gensler,

The Consumer Protection Division of the Office of the Attorney General (the "Division") enforces the Personal Information Protection Act, Md. Code Ann., Com. Law § 13-3401, *et seq.* (2013 Repl. Vol. and 2017 Supp.) ("PIPA"). In large data breaches with a national reach, we typically do this by joining a multistate investigation with other states. The Division's Identity Theft Unit interacts directly with consumers and helps them with issues related to identity theft and data breaches.

Notice of a Data Breach to Consumers

In examining how a data breach affects a consumer, the first issue we need to consider is whether or not consumers are actually aware that their data was breached. Too often, we believe that they are not. Currently, PIPA gives companies an option to provide either direct notice to each affected consumer, or provide generalized substitute notice. Md. Code. Ann., Com. Law. § 14-3504(e). Substitute notice means posting notice on the company's website, notifying statewide media, and emailing, if email addresses are known. (Md. Code. Ann., Com. Law. § 14-3504(e)(4) and (f)). Substitute notice is much less effective than direct notice, but companies often take that available route. People without internet access, people who do not watch the news, and people who simply do not believe reports apply to them may be at greater risk than if they had been directly notified. We saw evidence of this in the wake of the Equifax breach. Equifax first reported that 143.5 million social security numbers had been breached, and initially provided substitute notice. Later, it discovered that an additional 2.5 million people were impacted, and decided to send those 2.5 million people direct notice by mail. Our Identify Theft Unit received at least as many calls from consumers who received the follow up direct notice (sent to 2.5 million people) as calls from consumers following the initial substitute notice to the much larger group of 143.5 million people.

A potential legislative solution to this concern would be to remove the option of either direct notice or substitute notice, and instead require both.

Notice of a Data Breach to the Attorney General's Office

The next issue to consider is whether the Attorney General's Office is effectively hearing about breaches. Our Identity Theft Unit responds to a flurry of consumer calls following a breach. It needs to have adequate information about the breach to be able to effectively advise consumers. PIPA requires a company to notify the AG of a breach prior to notifying consumers, but provides no guidance about what that notice needs to contain. (Md. Code. Ann., Com. Law. § 14-3504(h)).

We have several concerns about the notices that we are receiving. The first relates to timing. PIPA requires notice "as soon as reasonably practicable, but not later than 45 days after the business concludes [its] investigation...." We have noticed that some companies have ignored the "as soon as reasonably practicable" language and have instead viewed 45 days as their deadline, waiting until the last minute to provide notice. We also have concerns with the substance of the breach notifications. *See* Attachment A (Sample breach notification). PIPA does not require notices to include the number of affected Marylanders. That information is necessary for us to understand the scope of the breach, and is readily available to the companies. Next, PIPA does not require a description of the breach. Many notices contain no useful description of the breach or how it occurred. This information would help us answer consumer questions, and help us determine whether to open an investigation into a breach. Finally, PIPA does not require a company to provide a sample of the notice letter going out to consumers. Without that, we are at a disadvantage when consumers call asking questions about it.

Potential legislative solutions would be to require breach notifications to the Attorney General to include: (1) the number of affected Marylanders[1]; (2) a specific description of the breach and its cause[2]; and (3) sample consumer notice letters[3]. We would also recommend providing a form breach notification letter for companies to populate.[4] That would get us the information we need, and also make compliance easier for small businesses. And finally, the time period for providing notice should be shortened from 45 days.[5]

Credit Monitoring

The next thing consumers are likely to hear about is credit monitoring. It has become standard for companies to offer one or two years of "free" credit monitoring after a breach.[6]

---

[1] Such a requirement exists in Alabama, Florida, Illinois, Montana, New Hampshire, Rhode Island, Vermont, and Washington.

[2] Such a requirement exists in Alabama, Florida, Louisiana, and North Carolina.

[3] Such a requirement exists in California, Florida, Montana, North Carolina, Oregon, Rhode Island, Virginia, and Washington state

[4] This already exists in Massachusetts.

[5] The European Union's General Data Protection Regulation (GDPR) and the New York Department of Financial Services Cybersecurity regulations requires notice within 72 hours of discovery of a breach. Puerto Rico requires notice within 10 days of discovery. And Colorado and Florida require notice within 30 days.

[6] Some states actually require a company to provide consumers with free credit monitoring after a data breach (e.g. California, Connecticut)

Credit monitoring can be a useful tool, but as offered, it has some significant limitations. First, if the breached data included social security numbers, criminals are unlikely to try to exploit the data for several years, which would be after the free monitoring has expired. Second, it does not stop identity theft. Consumers do not always understand the limitations, leading them into a false sense of security. If a new fraudulent account is opened in a consumer's name, a credit monitoring service may notify them, but it will not stop that account from being created. And credit monitoring will not stop other common forms of identity theft, such as tax fraud. Third, few people actually sign up for the service. Fourth, we need to monitor the terms of use of the credit monitoring products to ensure that companies are not inserting abusive terms, such as forcing consumers to agree to let the issuer sell their personal information, to market to them, to try to upsell them to the issuer's paid products, or to agree to forced arbitration. Fifth, consumers may feel pressure to purchase the product after the free term has expired.

Consumer Impact of a Data Breach

After a data breach, consumers are typically angry and concerned. Angry that a company failed to do its job in protecting them, and has imposed an affirmative obligation on that consumer to protect themselves going forward, and concerned about consequences that may last a lifetime.

With a payment card breach, the impact on consumers is typically the time and inconvenience of taking on the active burden to replace their cards, dispute fraudulent charges, and closely monitor their accounts going forward. In terms of out-of-pocket costs, the system does a good job of protecting consumers from financial impact, as long as the fraudulent activity is detected. Federal law requires the card companies to absorb most, if not all, of the liability, which is built into theor cost of doing business. Perhaps, reflective of that, they are doing a good job at identifying fraud. There are some differences for consumers depending on whether it was a credit card or a debit card that was breached. If a credit card number is stolen (but not the physical card), a consumer is not liable for any unauthorized use of their card. The same is true with a debit card, but only if they report the unauthorized transaction within 60 days of receiving their statement. The big difference between credit cards and debit cards is a practical one. If a consumer disputes a credit card charge as fraudulent, their card issues a credit and they are not out of pocket any money during the investigation. But with a debit card number, a thief can use that to clean out their checking and linked savings accounts. If that happens, they may be without access to those funds during the duration of the investigation. Identity theft victims should be able to get them refunded, but it will take time. As for new account fraud, consumers are not be liable for debts on new accounts created in their name, but it will take time and effort to clear it up, including any negative impact on their credit score.

Breaches involving social security numbers are a bigger concern. A social security numbers is a static identifier, meaning it does not change, and the compromise presents a long-term risk of identity theft. Thieves sit on this information. They might not use it for years after a breach. With a social security number and other of your personal information, a thief can apply for new credit cards or loans, buy a phone on a long-term payment plan, open utility accounts, create bank accounts, file for your tax refund, collect social security benefits, or get healthcare or medical services. If paired with a driver's license number, they can create a fake ID, and apply for a job, get insurance, or even commit crimes in your name.

We also have concerns with other types of information being breached. Companies collecting DNA are becoming increasingly popular. What if a breach exposed genetic information? Currently, that might not be a data breach under PIPA. It is not part of the definition of "personal information" within the meaning of the act. But such a breach would be of grave concern to consumers. They cannot change their DNA. Further, if I provide my DNA, I am also providing my relatives' DNA without their knowledge or consent. Such information could be used against consumers by insurance companies seeking to identify genetic predispositions to illness, employers seeking to determine whether potential employees would hurt their insurance premiums, and by law enforcement.

A potential legislative solution would be to expand the definition of Personal Information in PIPA to include genetic information.[7]

And on the topic of expanding the definition of Personal Information, we should also consider adding personal health information and activity tracking data. Devices like Fitbit are collecting an increasing amount of information about people's habits and daily lives. They collect information about exercise and fitness habits, location, diet, weight, and fertility cycles. People have a legitimate expectation of privacy about that sensitive information

What Can Consumers Do to Protect Themselves After a Breach?

To protect against existing account fraud, the best thing to do is to monitor accounts, and to alert institutions if there is any unauthorized activity. This can be paired with placing a fraud alert at a Credit Reporting Agency, which notifies creditors that they should try to verify a consumer's identity before opening a new account. New federal law extends the duration of an initial fraud alert from 90 days to 1 year.

To protect against new account fraud, consumers should consider placing security freezes. They prevent new accounts from being opened in a consumer's name. But they do not protect against existing account fraud, so consumers still need to monitor their current accounts.

Federal law, taking effect September 21, 2018, preempts our state security freeze law, which was just amended last session. Fortunately, the federal law provides free freezes, thaws, and temporary lifts. And many of the protections are the same as under our law. The freeze itself operates in the same way, and the process for placing, temporarily lifting, and thawing the freeze is the same. Both placement and removal of a freeze are actually faster under the federal law: 1 day (if requested by phone or electronic means), as opposed to 3 days under Maryland law. But the temporary lifting of a freeze is slower under federal law: 1 hour, as opposed to 15 minutes under Maryland law. The federal law also adds a harmful exception – while a consumer has a freeze on, a CRA may share their credit report with "any person using the information for employment, tenant, or background screening purposes." That was not possible under Maryland law.

In preempting the part of Maryland law governing freezes for protected individuals, the federal law eliminated several categories of protected individuals that Maryland had just added

[7] Illinois, for example, has already done that (740 ILCS 14/10).

by amendment last session: people 85 years old or older, service members, and people incarcerated in a Maryland correctional facility.

PIPA Loophole

Lastly, I'd like to mention a loophole in our notice law related to hard-copy breaches. A company is required to take reasonable steps to protect Personal Information in any form (Md. Code Ann., Com Law § 14-3503(a)). However, PIPA only requires a company to provide notice of a breach that involves "the unauthorized acquisition of computerized data" (Md. Code Ann., Com Law § 14-3504). So, theoretically, if a business printed out all of their customers' social security numbers and names and it was taken off of the receptionist's desk, it would not have to notify us or consumers.

Potential Legislative Solution: delete the word "computerized" in Md. Code Ann., Com Law §14-3504.

Thank you for your consideration of these matters.

Sincerely,

Richard L. Trumka Jr.
Assistant Attorney General
Office of the Maryland Attorney General

cc: Members of the Commission

ATTACHMENT A

Reinhart
Attorneys at Law

Reinhart Boerner Van Deuren s.c.
P.O. Box 2965
Milwaukee, WI 53201-2965

1000 North Water Street
Suite 1700
Milwaukee, WI 53202-3197

Telephone: 414-298-1000
Fax: 414-298-8097
Toll Free: 800-553-6215
reinhartlaw.com

March 28, 2018

SENT BY CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Attorney General Office
200 St. Paul Place
Baltimore, MD 21201

Dear Mr. Frosh: Re: **NOTICE OF DATA BREACH**

Fred Usinger, Inc. ("Usinger's") has been informed that its hosting service provider for its e-commerce website experienced a data security incident in which the credit or debit card information of a number of Usinger's customers appears to have been accessed and acquired.

Usinger's intends to mail a written notice of data breach within the statutorily required period to the affected Maryland residents.

For further information, please contact the undersigned or [redacted] Vice President of Finance of Usinger's, at [redacted] between 9:00 a.m. - 5:00 p.m. CST daily.

Sincerely,

Martin J. McLaughlin

39286028