STATE OF KANSAS
OFFICE OF THE ATTORNEY GENERAL

DEREK SCHMIDT
ATTORNEY GENERAL

MEMORIAL HALL
120 SW 10TH AVE., 2ND FLOOR
TOPEKA, KS 66612-1597
(785) 296-2215 • FAX (785) 296-6296
WWW.AG.KS.GOV

Testimony in Support of House Bill 2580

Presented to the Senate Committee on Financial Institutions & Insurance
By Attorney General Derek Schmidt

March 13, 2018

Chairman Longbine, Members of the Committee:

Thank you for this opportunity to testify in support of House Bill 2580, which would prohibit the Credit Reporting Agencies (i.e., Equifax, Experian, Transunion)("CRAs") from charging consumers for placing or lifting a "security freeze" that bars most third-party access to the consumer's information held by the CRA.

It's a very simple bill: Currently, the CRAs may charge up to $5 to most Kansans in order to "freeze" their credit information and another $5 each time a Kansans wishes to "thaw" his or her information in order to, for example, open a new credit account. To freeze accounts at all three of the main CRAs, that means a Kansan might have to pay $15 to place the freeze and must pay again each time the freeze is "thawed." This can become extremely costly – not to mention annoying.

The need for this change became apparent last year when the enormous data breach at Equifax came to light. Equifax reports that more than 145 million Americans – including about 1 million Kansans, one-third of our state's population – had their personal information exposed as a result of this single data breach. And this was extremely sensitive information – including name, date of birth, Social Security number.

This breach was an identity thief's dream.

This was not unprecedented. Other CRAs also have had information compromised, though with less public and media attention. The risk of harm to consumers is real – and virtually certain.

The consequences of these sorts of breaches will follow affected Kansans for the rest of their lives because of the type of information compromised. Social Security numbers last a lifetime.

So naturally, many Kansans are concerned and want to take steps to protect themselves and their identities. And some significant number of Kansans have responded by desiring to place a "security freeze" on their credit reports – so that even if an identity thief obtains their

information, it will be difficult or impossible to open bogus credit in their names because of the freeze.

To be sure, many Kansans chose to protect themselves through other steps, services or actions. Attached is an article from Consumer Reports that discusses various options. But security freezes are a top choice for many because, while inconvenient, they are the most effective option to prevent unauthorized use of a consumer's credit report. And it seems to me that, as a matter of public policy, we should reward those Kansans who choose the most effective method of preventing access to their credit accounts – not punish them by charging them a fee for protecting themselves.

In the months after the Equifax breach became public, one of the most common complaints to my office was this: "I did not cause my personal information to be collected by Equifax. I did not cause Equifax to be breached. So why must I pay to prevent identity thieves from using it against me?"

That seems to me a quite reasonable question.

Kansas already prohibits the CRAs from charging a fee to place or lift a security freeze on the account of a person who is a victim of identity theft. It seems to me reasonable to allow this same treatment before the horse is out of the barn, so to speak, and make no-fee security freezes and thaws available to any Kansans who want to protect against identity theft in this way.

This proposal for no-fee security freezes and thaws is in effect elsewhere. At least five states and the District of Columbia already prohibit the credit reporting agencies from charging any fee in order to place or lift a security freeze: Indiana, Maine, Maryland, North Carolina, South Carolina and the District of Columbia. The U.S. Congress is considering legislation to make this federal policy.

Enactment of House Bill 2580 would add Kansas to that list. It seems to me fundamentally fair – the right thing to do – to do so. I encourage you to adopt this measure, and I would stand for questions.

###

Equifax Data Breach Was Bigger Than Previously Reported

But consumers may not be at greater risk than before, security expert says

By Octavio Blanco
February 09, 2018

Equifax hackers reportedly accessed more personal information than previously disclosed, but the additional breach may not have put consumers at more risk than they already are, a cybersecurity expert says.

The credit rating agency, which disclosed the massive hack in September, reported the additional breaches in documents submitted to the Senate Banking Committee, the Wall Street Journal reported Friday.

In addition to the data that had previously been disclosed, hackers were able to access "tax identification numbers, email addresses and drivers' license information beyond the license numbers," the Journal said.

More than 145 million Americans were affected by the Equifax hack last summer. The personal information accessed–which included Social Security numbers, driver's license numbers, and credit card numbers–would allow criminals to steal a consumer's identity and open fraudulent accounts.

While alarming, the disclosure that additional personal information was accessed doesn't necessarily put consumers at more risk than before.

"This is negative news, and it doesn't look good for Equifax,"

says Al Pascual, senior vice president and research director at Javelin Strategy & Research. “But considering the scale of the breach, this additional information doesn’t move the needle. If the additional data is encompassed within the 145 million people originally impacted, then it’s not something to be concerned about.”

An Equifax spokeswoman, Meredith Griffanti, told Consumer Reports that the Journal headline on the article—“Equifax Hack Might Be Worse Than You Think”—was “extremely misleading.”

She added that the “approximately 145.5 million consumers (affected by the data breach) has not changed.”

Consumer advocates, however, said this latest disclosure showed just how much personal information is collected by Equifax and other credit rating agencies, making all consumers vulnerable to identity theft.

“This is a demonstration of the broad array of personal information that Equifax holds about nearly every American, and a reminder of the need for individuals to protect themselves following the breach,” says Anna Laitin, director of financial policy at Consumers Union, the advocacy division of Consumer Reports. “If consumers haven’t yet put a freeze on their credit report, now is as good a time as any to do so.”

There are several ways you can protect yourself.

Place a Freeze on Your Credit File

A security freeze placed on your credit file will block most lenders from seeing your credit history. That makes a freeze the single most effective way to protect against fraud.

If a prospective lender can't pull your credit report, he won't issue a new loan. That usually stops identity thieves from setting up fraudulent accounts in your name.

There's a drawback, though. The freeze also shuts out most companies you may want to do business with, including lenders, telecom companies, and insurers.

To give them access when you want to apply for a loan or open a cellular service account, you have to temporarily lift the freeze and set a date for it to be reinstated automatically.

If you've already been the victim of identity theft, a less restrictive option is a fraud alert, which is a notice placed on your credit report that lets prospective lenders know that you are a victim of identity theft and that they should take reasonable extra steps to verify your identity before granting credit to the person claiming to be you.

While a credit freeze offers far more protection than a fraud

alert, banks and credit unions where you already have accounts can still check your credit report, as well as collection agencies and certain government agencies.

A freeze might be free, depending on your state and circumstances–for example, if you're an identity-theft victim and have filed a police report about the incident. Otherwise, expect to pay $2 to $12 to initiate or temporarily lift a freeze at each credit bureau: Equifax, Experian, TransUnion, and Innovis. Review your state's law for details.

Consider a Credit Lock

Like a credit freeze, a credit lock, a service all three major credit bureaus provide, prevents someone from opening a credit account in your name. But although credit locks and freezes do the same thing, there are some important differences between the two.

First, there's the question of speed and convenience. A credit lock, which you initiate using an app on your smartphone, generally happens right away. Activating and lifting a security freeze can be a little more time-consuming. The credit bureaus say they need 24 to 48 hours to process the request.

There are also cost considerations. Only two credit monitoring bureaus, TransUnion and Equifax, offer free credit-lock products. Experian offers a subscription-based credit lock product called CreditLock through CreditWorks, but it costs $5 for the first month of access and $25 per month thereafter.

Locking down only two of your three main credit reports isn't enough. Experts say you have to lock all three.

Another difference between a lock and a freeze: The latter offers stiffer protections. A credit freeze's promise to guard your credit accounts is guaranteed by law. By contrast, a credit lock is simply an agreement between you and the credit monitoring company. Having a contractual agreement is not as strong as having protections under law.

Activate Two-Factor Authentication

In today's world of digital crime and internet fraud, two-factor authentication is an important extra layer of safety. It requires not just a password but also a second element, such as a code texted to your smartphone, which *you* have but a crook can't easily get. Set up and activate two-factor authentication on all your existing mobile banking, savings, credit card, home equity line of credit, and other financial accounts that offer it.

Most banks that offer mobile banking also authenticate the device you use to access your account. Banks with the most cutting-edge security use yet another factor, biometric authentication, which verifies your identity by using your fingerprint or voice print, or through facial recognition–which criminals can't easily fake.
