Christopher_FAV_SB160
Uploaded by: Anonymous, Christopher
Position: FAV

SB0160/HB0247: Financial Institutions - Security Questions and Measures
February 4, 2020 – FAVORABLE REPORT

Christopher
Debary, Florida

My name is Christopher. I'm an American citizen residing in Debary, Florida. I prefer that my complete identity remain anonymous. I am a victim of fraud directly related to the "security and recovery methods" imposed by my financial institutions' requirement of providing my mother's maiden name. I felt it important to share my story with you. I have learned, the hard way, it is not an uncommon story.

I was very happy to hear about **SB0160 (HB0274).**

It is imperative that financial institutions adopt more stringent requirements in their current password recovery systems: more specifically, the removal of "your mother's maiden name" fields within the security and recovery methods.

In today's world of free information gathering across the Internet, requesting a person's mother's maiden name is flawed and outdated. The information is so easily gained by simple search engine methods.

This past spring, as I would start my day on any Saturday, I turned on my cell phone and tablet to read my e-mail and catch up on news. Nearly immediately, I started to receive text messages about account activity with my checking and savings accounts as well as my credit card held with another bank. I was hacked! How could this have happened? I followed security measures required by the banks, I am a responsible user of the internet and e-mail servers. I am aware and very cautious of "phishing scams."

I immediately signed into the respective accounts to find zero balances. Panic set in and I called the banks… this is where the trouble truly starts.

I learned that the hacker(s) had used my mother's maiden name to gain access to my email account. From the email account, they were able to intercept communication from my banks without my knowledge. They had access to everything! Overnight, they password reset my accounts using my email address and the single step security measures.

I called the credit card company and was met with hesitation and skepticism as they paid the small balance carried on the card, and with my own checking account they overpaid the credit card. Within the credit card "rules," if an overpayment is received, it will create negative debt,

or a “credit balance.” You can do nothing, and in 30 days or one billing cycle, the bank carrying the credit memo will return your account to “$0” by issuing a paper check. The other option is to spend your way out of the credit memo by charging the card up to or beyond “$0.” My card was used at a high-end online retailer to purchase home goods and furnishing. Both banks placed stops on the accounts, initiated their individual protocols, and reissued credit cards, bank card, etc.

The security question, and recovery email were not updated. E-mails were sent and cards were replaced. Unrealized at the time, the new information was being intercepted. The “hackers” were repeating the process before the new cards were ever received in the mail! I had to go through the same situation time and again. Texts, banks, phone calls, skepticism etc.

Through the experience, I realized I too had access to my accounts, I could see exactly when, and with what company, my money was being used to fraudulently purchase home goods. So, I called. I was given immediate access to the invoices and could see all the shipping details and products being purchased. Sure enough, my card has been recorded, and the product was being delivered to two different addresses, one in New Hampshire and one in Oregon. The only thing I couldn’t do was request refunds or to stop shipment as my name was not the shipper’s name and that, of all things, couldn’t be shared.

I called the banks yet again and informed them that I went sleuthing and found out who had defrauded them/me. I tried to give them the addresses and copies of the invoices, but they refused the information. I also told them through my investigations I learned that my email address was the root source of everything and had since closed that account, deleted its 15-year history, and had purchased a replacement computer without backing it up. I had officially started over! 41 years old and I had to start my “E-world” from scratch.

Another problem: I knew my mother’s maiden name of course, and I knew the old email address but because an account alert had been set and they were currently “investigating” a claim, I couldn’t make any changes whatsoever to my accounts. “The banks” were required to send the information to the e-mail address on file. The same e-mail address that the hackers had access to for the next 72 - 96 hours (that’s how long the data exists on this particular server once a request to delete the email address occurs. This is a safety protocol established in case the user didn’t mean to request or changed their mind and wished to keep the e-mail account active.)

It took five representatives, their supervisors, and two Sr. team members to convince them that the protocol needed to be overridden to prevent the problem from occurring again. I had to threaten my business with these companies to facilitate this needed action. The banks finally saw my point of view and delivered. We finally were on track! Money was replaced and

ultimately, I was not held responsible. My nerves were shot. The ordeal left me financially whole, but only after weeks of financial torture.

I learned valuable lessons. The banks, it seems, are uninterested in perusing anything further for fraudulent charges totaling $24,999 or less. I'm not an economist, but I am sure this is costing the American taxpayer billions annually. Interest rates must be affected as well; how else could the bank afford to "wipe the slate clean" on these types of charges with their zero risk policies?

No matter how secure we as consumers think our accounts are, or how careful we are in meeting security protocol, there is always a single question that can unravel everything, creating unnecessary financial strain and stress on the average American citizen.

Financial institutions across the nation need to protect themselves and their customers by implementing more stringent security protocol, by removing question samples such as "your mother's maiden name" and creating a system of personalized unique identifiers created upon the opening of said account.

The change in technology would, I assume, be a financial investment with an upfront cost, but the billions saved annually by fewer claims being reported surely outweighs this initial investment.

If the banks refuse to take action of their own volition and self-preservation, then I call on our elected officials to facilitate this change by enacting law specifically designed to protect customers from fraud. You must hold these institutions responsible; we can't afford not to.

"What is your mother's maiden name" - six words I wish I never had to see again.

Global_Investigative_Services_FAV_SB160
Uploaded by: Mack, Linda
Position: FAV

GLOBAL
INVESTIGATIVE SERVICES
Safe. Fast. Affordable.

SB0160-FAVORABLE

Good Afternoon,

Chairperson Kelley and members of the Finance Committee.

My name is Linda Mack, I am President and CEO of Global Investigative Services, Inc. a licensed private investigator and accredited consumer reporting agency located in Rockville, Maryland.

I write to you today to ask that you find in favor of **SB0160**

Requiring a financial institution that requires a customer to provide an answer to a security question for a certain purpose to allow a customer to choose from at least two options for each required security question; and prohibiting a financial institution from using a customer's mother's maiden name as a means of safeguarding access to the customer's account.

Your mother's maiden name is not a secret. This should be obvious, yet this question and similarly flawed questions continue to be asked of us when we forget a password or log in from a new computer.

Website security questions have been around since the dawn of the web but became ubiquitous after a 2005 recommendation by the Federal Financial Institutions Examination Council that banks improve their security measures for online banking. The council did not specify what these improvements should be, and so banks chose security questions, something they had been using offline for decades anyway — the mother's maiden name convention dates to 1882. Other types of businesses, perhaps assuming that the banks knew what they were doing, followed suit.

Security questions are astonishingly insecure: The answers to many of them are easily researched or guessed, yet they can be the sole barrier to

1700 Rockville Pike • Suite 230 • Rockville, MD 20852 • Toll Free 1-800-589-6595 • Fax (301) 589-6055

someone gaining access to your account. Still, this has persisted despite the availability of two-factor authentication and persisted on sites that we use frequently and that contain important, sensitive data – banks, airlines, Facebook, Amazon, PayPal.

As long as security questions are going to be used, professional consensus holds, they should have many possible answers, and each of those possible answers should be simple, stable, memorable and not easily researched or guessed.

When people use their mother's real maiden name so that they are sure they can remember what to provide when asked (e.g. as part of the process to recover the account). This means that this is information is fixed for a very long period of time. If it happens that some web application is hacked and such an answer is associated with an e-mail address (or worse, with personally identifiable information), it can potentially create a vulnerability for other web applications.

The temporary solution is to create false answers and to keep them somewhere safe, whether in a password manager (which can generate and store a random string for each answer field) or even on a piece of paper.

The permanent solution is to remove these questions entirely, specifically, "what is your mother's maiden name?" and replace the current security and recovery methods with a more secure method, such as a two-factor authentication.

Thank you for allowing me to offer my opinion to this committee. If you have any questions or need additional information, please contact me at lbm@gispi.com or by phone at 301-589-0088.

MDPIRG_FAV_SB160
Uploaded by: Scarr, Emily
Position: FAV

SB160: Financial Institutions - Security Questions and Measures
Senate Finance Committee
February 4, 2020, 1:00 PM

FAVORABLE

Maryland PIRG is a state based, non-partisan, citizen funded public interest advocacy organization with grassroots members across the state and a student funded, student directed chapter at the University of Maryland College Park. For forty five years we've stood up to powerful interests whenever they threaten our health and safety, our financial security, or our right to fully participate in our democratic society. ***That includes a long history of working to protect consumers from identity theft.***

SB160 requires banks to provide at least two options for security questions. As amended by the sponsor, it also stops banks away from using "mother's maiden name" as a security question for new accounts.

Both of these common sense measures will help protect Marylanders from "Existing Account Fraud" by making it harder for identity thieves to access their bank accounts.

There is nothing we can do to make consumers entirely free of risk of identity theft, but smart public policy and common sense consumer actions can significantly reduce risk.

We recommend Marylanders don't show personal information on social networking sites that are commonly used to verify your identity, such as date of birth, city of birth, mother's maiden name, name of high school, etc. Or if they do, they shouldn't use that information to verify their identity with banks or other accounts. We include this, and other tips with our Identity Theft Protection Guide: https://marylandpirg.org/issues/usf/protecting-yourself-identity-theft.

Thanks for your service to Maryland, we respectfully request a favorable report on SB160.

emily@marylandpirg.org
@emilyscarr

Senator_Kagan_FAV_SB160
Uploaded by: Senator Kagan, Senator Kagan
Position: FAV

CHERYL C. KAGAN
Legislative District 17
Montgomery County

Vice Chair
Education, Health, and
Environmental Affairs Committee

Joint Audit Committee
Joint Committee on Federal Relations

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Miller Senate Office Building
11 Bladen Street, Suite 2 West
Annapolis, Maryland 21401
301-858-3134 · 410-841-3134
800-492-7122 *Ext.* 3134
Fax 301-858-3665 · 410-841-3665
Cheryl.Kagan@senate.state.md.us

SB160: Financial Institutions - Security Questions and Measures
Senate Finance Committee
February 4, 2020, 1:00 PM

Using a mother's maiden name as a security question dates back to 1882. This made sense when most women changed their names after marriage, but society has changed. Many women retain their maiden names after marriage; honor their mothers with hyphenated names, and people with LGBTQ parents may have two fathers meaning this question is not even applicable. Additionally, the Internet has made personal information increasingly available.

Nevertheless, some banks continue to use mother's maiden name as a security measure and don't offer alternatives. This archaic approach to protecting account holders' information leaves it vulnerable to hacking. In 2005, researchers from Indiana University Bloomington were able to use public records to deduce the name of 4,105,111 Texans-- 18% of the State's total population. The increased use of social media has made family relations easy to identify, making this information even more accessible to criminals.

SB160 would simply require banks to provide at least two security questions-- neither of which can ask for a mother's maiden name. In addition, I am offering a clarifying amendment that would ensure this bill is **prospective and not retrospective.** These common-sense parameters will help protect account holders from hackers.

I urge a favorable report on SB160 with a clarifying amendment.

Gigi Godwin_FWA_SB 160
Uploaded by: Godwin, Gigi
Position: FWA

To Lead, Advocate and Connect as the Voice of Business

Senate Bill 160 - Financial Institutions – Security Questions and Measures

Finance Committee

February 4, 2020

SUPPORT WITH AMENDMENT

Senate Bill 160 requires a financial institution to allow a customer to choose from at least two options for each security question if the customer is required to provide an answer to a security question in connection with the provision of an account. The bill also prohibits a financial institution from using a customer's mother's maiden name as a means of safeguarding access to the account.

The Chamber supports the first portion of the bill; more than one option for a security question ensures the consumer is able to choose a question that best suits their individual needs. However, the prohibition of the use of a mother's maiden name is unnecessarily burdensome and has potential legal ramifications.

There is a concern that this bill could only pertain to State Chartered Banks, as Federal Chartered Banks follow the rules of the federal government. This prohibition could potentially cause issues with not only banks, but credit card companies, and other Federal Chartered Institutions. Finally, there is a cost associated with this prohibition as banks, credit card companies, and others, would have to change the security questions on their respective websites.

For the aforementioned reasons, **the Chamber supports Senate Bill 160 with an amendment and respectfully urges a favorable report.**

The Montgomery County Chamber of Commerce (MCCC) accelerates the success of our nearly 500 members by advocating for increased business opportunities, strategic investment in infrastructure, and balanced tax reform to advance Metro Maryland as a regional, national, and global location for business success. Established in 1959, MCCC is an independent non-profit membership organization and is proud to be a Montgomery County Green Certified Business.

Tricia Swanson, Vice President, Government Relations
Montgomery County Chamber of Commerce
301-738-0015 www.mcccmd.com

MBA_FWA_SB160
Uploaded by: Murphy, Kathleen
Position: FWA

Senate Bill 160 – Financial Institutions – Security Questions and Measures

Senate Finance Committee

February 4, 2020

Favorable with Amendments

The Maryland Bankers Association (MBA) supports Senate Bill 160 – Financial Institutions – Security Questions and Measures with amendments. This legislation requires a financial institution to allow a customer to choose from at least two options for each security question if the customer is required to provide an answer to a security question in connection with the provision of an account. The bill also prohibits a financial institution from using a customer's mother's maiden name as a means of safeguarding access to the account.

MBA members expend significant measures to safeguard their customers' accounts from unauthorized access. Use of a security question is frequently one of the protocols used to verify that the person inquiring about the account is actually the person who owns the account. We appreciate the intent of the legislation and support the requirement in the bill that if a financial institution requires a customer to provide an answer to a security question, the customer shall be given the option to choose from at least two options.

MBA respectfully requests the following amendments:

Strike 1-212 (B) beginning on page 1 line 22 through line 24– MBA requests that the bill be amended to remove the prohibition on the use of a mother's maiden name as an answer to one of the security questions. Removing the ability to use a mother's maiden name eliminates a popular option that is widely offered today. Maryland would be the only state with this prohibition. With a requirement that at least two security question options be provided, the customer can choose not to use the mother's maiden name as the answer to their security question.

The banking industry strongly supports security measures to safeguard customers' access to their bank accounts. It is important that measures used are easily remembered and do not cause undue frustration for bank customers when inquiring about their accounts.

Extend the effective date to January 1, 2021 – Banks will need to reconfigure their systems to comply with the requirement to provide at least two security question options. Extending the effective date will enable this to occur.

With these amendments, MBA supports Senate Bill 160.

MD DC CUA_UNF-SB160
Uploaded by: Murray, Rory
Position: UNF

MD|DC
Credit Union Association

Engage • Influence • Impact

Chair Delores Kelley
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

SB160: Financial Institutions - Security Questions and Measures
Testimony on Behalf of: MD|DC Credit Union Association
Position: Oppose

Chairwoman Kelley, Vice-Chair Feldman and Members of the Committee:

On behalf of the MD| DC Credit Union Association and the 84 Credit Unions and their 1.9 million members that we represent in the State of Maryland, we appreciate the opportunity to testify on this legislation. Credit Unions are member-owned, not-for-profit financial cooperatives whose mission is to promote thrift and provide access to credit for provident and productive purposes for our members. We respectfully oppose this bill.

As a general matter, the safety of our members comes first, and credit unions take great care to protect member data. The language in this bill reflects the standard practice in the financial services industry. Credit union members are generally provided with two or more security questions to choose from and many credit unions do not have "what is your mother's maiden name" as an option. However, this bill is problematic for credit unions because we rely heavily on vendors to provide many of the security platforms and services used by the members. If a vendor serves credit unions in multiple states and must modify their platform in the State of Maryland, as this bill may require, it could increase the costs to credit unions, or the vendor may decide not to conduct business in Maryland at all.

We fully understand the intent of the legislature with the introduction of this bill; however, we do not think that business decisions should not be micromanaged by statute. It is one thing to require that credit unions implement policies and procedures that protect their members and require supervision and examination, as is the current law. It is a more concerning level of micromanagement to pick and choose what questions are appropriate for financial institutions to use to protect data.

Credit unions are subject to strict standards pertaining to data protection, and our consumer-facing data platforms are included in the examinations. If an examiner determines that our standards do not sufficiently protect our members, they may issue a prompt corrective action order; an order to cease and desist, which requires a party to take action (or refrain from taking action), including making restitution; an order assessing civil money penalties; documents of resolution, letters of understanding or; agreement or consent order.

8975 Guilford Road, Suite 190, Columbia, MD 21046
P 443-325-0774 C 410-980-9275
F 410-290-7832 E jbratsakis@mddccua.org
mddccua.org

MD|DC
Credit Union Association

Engage · Influence · Impact

Due to our close working relationship, we think it is more appropriate for our primary regulators to issue guidance on these types of issues as they deem necessary.

Please do not hesitate to contact me at 443-325-0774 or jbratsakis@mddccua.org, or our VP of Advocacy, Rory Murray at rmurray@mddccua.org should you have any questions. Thank you for your consideration.

Sincerely,

John Bratsakis
President/CEO
MD|DC Credit Union Association
8975 Guildford Rd., Suite 190
Columbia, MD 21046