EPIC-MD-SecurityQuestions-Feb2021.pdf
Uploaded by: Fitzgerald, Caitriona
Position: FAV

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 5, 2021

The Honorable Dolores G. Kelley, Chair
Senate Finance Committee
Maryland General Assembly
3 East
Miller Senate Office Building
Annapolis, MD 21401

Dear Chair Davis and Members of the Committee:

EPIC writes in support of Senate Bill 185 regarding financial institutions' security questions and measures. SB185 would help protect Marylanders from identity theft by requiring financial institutions who choose to use security questions to provide customers with more than one security question option.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has long advocated for cybersecurity safeguards for consumer information held by financial and commercial organizations. EPIC has previously testified before Congress on the need for financial institutions and companies to protect consumers against data breaches.[1]

Security Questions are a Poor Security Measure

We're all familiar with the situation: you create an online account, set a password, and the site asks you to answer one or more "security questions" in case you need to reset your password or verify your identity. The problem? The answer to many of those security questions is not secret. Yet many financial institutions are using these questions as a critical identity verification method that gives access to an account. But there are much more secure authentication techniques now widely available. And the use a weak security question undermines complex password requirements and other security precautions. The requirement that your password contain one uppercase letter, one uppercase letter, one symbol, and one number is meaningless if all that is required to bypass that password is your pet's name.

[1] *See, e.g.*, *Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the H. Comm. on Financial Services*, 115th Cong. (2018) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf; *Consumer Data Security and the Credit Bureaus: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. (2017) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/testimony/congress/EPIC-Testimony-SBC-10-17.pdf; *Cybersecurity and Data Protection in the Financial Services Sector: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 112th Cong. (2011) (statement of Marc Rotenberg, Exec. Dir., EPIC), https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.

During the 2008 U.S. Presidential election campaign, Vice Presidential candidate Sarah Palin's personal Yahoo email account was hacked by a 20-year-old college student who looked up the answers to her security questions—such as her birthdate and high school—and subsequently changed her password and gained access to her e-mail account.[2] In 2005, Paris Hilton's T-Mobile account was improperly accessed by a teenager who did a quick online search for "Paris Hilton Chihuahua" and therefore could answer the "secret question" of "what is your favorite pet's name."[3] These so-called "social engineering" attacks pose a significant risk to accounts that do not have strong verification standards.

The question of "what is your mother's maiden name?" is possibly the least secure of all security question options. Your mother's maiden name may in fact be your last name. But even if it is not, it is easily discoverable through an internet search, listed in obituaries, wedding and birth announcements, and social media posts.[4] Financial institutions should not even offer this question as an option, but at minimum they must offer other options, as SB185 requires.

The weakness of security questions as an authenticator has been known for years. Sixteen years ago, renowned security expert and Lecturer in Public Policy at the Harvard Kennedy School Bruce Schneier wrote "The answer to the secret question is much easier to guess than a good password, and the information is much more public."[5] In June 2017, the National Institute of Standards and Technology ("NIST"), which operates under the U.S. Department of Commerce, updated its Digital Identity Guidelines and removed its previous recommendation for security questions as an authenticator.[6]

Best Practices for Authentication

There are plenty of alternative authentication methods available today. Financial institutions truly should no longer be using basic security questions. EPIC recommends that institutions should follow the best practices laid out in NIST's Digital Identity Guidelines.[7]

But if security questions are going to be used, institutions should ensure that multiple question options are given, and that users are permitted to answer the questions with randomly-generated password-like answers rather than factual, semantic answers. This allows users who use a password manager to store those answers with their account information and prevent hackers from guessing those answers.

---

[2] Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED (Sept. 2008), https://www.wired.com/2008/09/palin-e-mail-ha/.
[3] Anne Diebel, *Your Mother's Maiden Name is Not a Secret*, N.Y. Times (Dec. 28, 2017), https://www.nytimes.com/2017/12/28/opinion/sunday/internet-security-questions.html.
[4] *Id.*
[5] Bruce Schneier, *The Curse of the Secret Question* (2005), https://www.schneier.com/essays/archives/2005/02/the_curse_of_the_sec.html.
[6] Nat'l Institute of Standards and Tech., U.S. Dept. of Commerce, *NIST Special Publication 800-63B: Digital Identity Guidelines* (June 2017), *available at* https://pages.nist.gov/800-63-3/sp800-63b.html#sec5; Lily Hay Newman, *Time to Kill Security Questions—or Answer Them With Lies*, WIRED (Sept. 28, 2016), https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/.
[7] *Id.*

By requiring that financial institutions who choose to use security questions to provide customers with more than one security question option, SB185 is a step in the right direction in protecting Marylanders against identity theft. The Committee should give SB185 a favorable report.

If EPIC can be of any assistance to the Committee, please contact EPIC Policy Director Caitriona Fitzgerald at fitzgerald@epic.org.

Sincerely,

/s/ *Alan Butler*
Alan Butler
EPIC Interim Executive Director
and General Counsel

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Interim Associate Director and
Policy Director

SB185_ Mother's Maiden Name Testimony - Sen. Chery
Uploaded by: Kagan, Sen. Cheryl
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

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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

SB185: Financial Institutions - Security Questions and Measures
Senate Finance Committee
Tuesday, February 9, 2021 | 1:00 PM

Using your mother's maiden name as a security question dates back to 1882. This was normal when most women changed their names after marriage, but society has evolved. Today, many women retain their maiden names after marriage or honor their mothers with hyphenated names. Individuals with LGBTQ+ parents may have two fathers, meaning this question is not even applicable. Additionally, the Internet has allowed for personal information to become increasingly available.

Nevertheless, some banks and other institutions continue to require "What is your mother's maiden name?" as a security measure and do not offer alternative options. This archaic approach to protecting account holders' information leaves their life savings 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 for malicious purposes.

Last year's SB160/HB274, which passed in the House, would have **eliminated** "What is your mother's maiden name?" as a bank security question. This year, SB185/HB471 would simply require banks to provide an alternative option. Consumers would have the choice of providing their mother's maiden name **OR** select another question they find more secure. After meeting with the Maryland Bankers Association in the interim, we decided that moving forward with the bill as written *now* would provide sufficient protection while also taking into consideration industry wishes.

This bill is **prospective and not retrospective.** These common-sense parameters will help give bank account holders reasonable options to protect them from hackers.

I urge a favorable report on SB185.

GR 21 - SB 185- MBA written testimony - Security Q

Uploaded by: Lehman, Mindy

Position: FAV

Senate Bill 185 – Financial Institutions – Security Questions and Measures

Senate Finance Committee

February 9, 2021

Support

The Maryland Bankers Association (MBA) represents FDIC-insured community, regional and nation-wide banks that employ more than 26,000 Marylanders and hold more than $182 billion in deposits in over 1,400 branches across our State. The Maryland banking industry serves about 6 million customers across the State and provides an array of financial services including residential mortgage lending, business banking, estates and trust services, consumer banking and more.

The Maryland Bankers Association (MBA) supports Senate Bill 185 – Financial Institutions – Security Questions and Measures. 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.

MBA members expend significant efforts 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.

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.

MBA encourages a favorable committee report on SB 185.

Testimony-SB0185 HB0471 Linda Mack.pdf
Uploaded by: Mack, Linda
Position: FAV

SB 0185/ HB0471- Favorable

Good Afternoon,

Chairperson Kelley and members of the Finance Committee.

My name is Linda Mack and I am President and CEO of Global Investigative Services, Inc. a licensed private investigative company and Accredited consumer reporting agency located in Montgomery County, Maryland.

I write to you today and request the you find favorably to **SB0185/HB0471.**

Requiring a financial institution that requires a customer to provide an answer to a security question in connection with the provision of an account to allow a customer to choose from at least two security questions options for each required security question; and applying the Act prospectively.

The answers to the most common security questions, such as, **"mothers maiden name"** are not a secret. This should be obvious, yet this question and similarly flawed questions continue to be asked when we forget a password or log in to a new computer.

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

Security questions are astonishingly insecure: The answers to many of them can be easily researched or guessed yet they can be the sole barrier to someone gaining access to your accounts. Still this has persisted despite the availability of more secure methods such as **two factor authentication** and persisted on sites we frequent such as our banks, airlines, Facebook, Amazon and PayPal.

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

When people use real answers to questions such as: **What is your mother's maiden name**? This information is fixed for a very long period of time. If it happens that some web application is hacked and associated with an email address (or worst with personal identifying information) it can potentially create a vulnerability not only to the user, but other web applications.

The temporary solution is to create false answers and to keep them somewhere safe, whether on 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 and replace the current security and recovery methods with a more secure method such as two factor authentication.

Thank you for allowing me to offer my opinions to the committee. If you have any questions or would like additional information, please contact me at lbm@gispi.com or by telephone at 301-589-0088.

SB185_MCRC_FAV.pdf
Uploaded by: Stern, Isadora
Position: FAV

Maryland Consumer Rights Coalition

Testimony to the Senate Finance Committee
SB 185 Financial Institutions - Security Questions and Measures
Position: Favorable

February 9, 2021

The Honorable Delores Kelley, Chair
Senate Finance Committee
3 East, Miller Senate Office Building
Annapolis, Maryland 21401
cc: Members, Senate Finance Committee

Honorable Chair Kelley and Members of the Committee:

The Maryland Consumer Rights Coalition (MCRC) is a statewide coalition of individuals and organizations that advances financial justice and economic inclusion for Maryland consumers through research, education, direct service, and advocacy. Our 8,500 supporters include consumer advocates, practitioners, and low-income and working families throughout Maryland.

We are writing today in support of SB 185.

SB 185 will increase consumer security by requiring a financial institution to allow a customer to choose from at least two security question options for each security question. While security questions have become an intrinsic part of today's web-based information management, their history stretches back more than a hundred and fifty years. Originally implemented in New York in 1850 by Emigrant Industrial Savings Bank, the security question had been adopted widely in the US banking sector by the turn of the twentieth century.[1] Many of the same questions developed in the mid-nineteenth century are still used today. However, with increased access to online data and social media, those same questions do not offer the security they did in the eighteen hundreds.

Security questions are an important barrier between consumers' private information and predatory hackers and scammers. MCRC's Securing Older Adult Resources (SOAR) program provides older adults in Maryland with financial coaching and counseling, as well as digital privacy training. Older adults are vulnerable to fraud and scams because of their lack of digital literacy. Collectively, older adults lose as much as $36 billion annually to financial exploitation. Unfortunately, fraud and scams are on the rise as scammers take advantage of the fear that the COVID-19 pandemic is causing[2].

[1] https://ourglasslake.com/wp-content/uploads/2018/02/Ruberg-FMH-Mother-Maiden-Name-July-2017.pdf
[2]

Maryland Consumer Rights Coalition

Supporting SB 185 would add protections for vulnerable consumers by updating the antiquated security question system. This increase in security is vital in this digital age, and the need has become exacerbated due to the increase in COVID-19 related fraud and scams.

For these reasons, we support SB 185 and ask for a favorable report.

Best,

Isadora Stern
Economic and Tenants' Rights Organizer
Maryland Consumer Rights Coalition

https://www.cnbc.com/2017/08/25/elder-financial-fraud-is-36-billion-and-growing.html#:~:text=One%202015%20report%20estimated%20that,a%20segment%20of%20the%20victims.

SB185 - 2021 - MDDCCUA- Financial Institutions - S

Uploaded by: Murray, Rory

Position: INFO

MD|DC
Credit Union Association

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

SB185: Financial Institutions - Security Questions and Measures
Testimony on Behalf of: MD|DC Credit Union Association
Position: Informational Testimony Only

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

The MD|DC Credit Union Association, on behalf of the 77 Credit Unions and their 2.2 million members that we represent in the State of Maryland, appreciates the opportunity to testify on this legislation. Credit Unions are member-owned, not-for-profit financial cooperatives whose mission is to educate and help members achieve financial well-being.

We do not oppose this bill's substance, as it won't likely affect our members; however, we would caution the General Assembly against passing laws of such a granular nature. Items of such specificity should remain under the regulator's purview, who has more flexibility to make rules and decisions related to the adequacy of the standards implemented in every aspect of the credit union. Regulators are subject matter experts who possess detailed knowledge about how the industry they regulate operates. Under the current framework, credit unions are subject to strict supervision and examinations on data protection, and our consumer-facing data protection platforms are included in the examinations. If an examiner determines that our standards do not sufficiently protect our members, they may implement new rules, issue a prompt corrective action order, an order to cease and desist, or several other protective measures.

In the small chance that this bill does pose a problem for a credit union, because they may rely on a vendor to provide this service, the regulator would be the appropriate decision-maker as to how the credit union should proceed. For the sake of flexibility and discretion in the supervisory process, we request that any issues that are this specific be left to the regulator.

Please reach out to me at jbratsakis@mddccua.org or our VP of Advocacy, Rory Murray, at rmurray@mddccua.org with comments or questions.

Thank you!

Sincerely,

John Bratsakis
President/CEO
MD|DC Credit Union Association