EPIC-MD-SecurityQuestions-Mar2022.pdf
Uploaded by: Caitriona Fitzgerald
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

March 8, 2022

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 639 regarding financial institutions' security questions and measures. SB639 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 of a weak security question undermines complex password requirements and other security precautions. The requirement that your password contain one uppercase letter, one lowercase letter, one symbol, and one number is meaningless if all that is required to bypass that password is your mother's maiden 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 SB639 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, SB639 is a step in the right direction in protecting Marylanders against identity theft. The Committee should give SB639 a favorable report.

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

Sincerely,

Caitriona Fitzgerald
EPIC Deputy Director

SB0639 - Letter to Legislators.pdf
Uploaded by: Marc Linchuck
Position: FAV

Global
INVESTIGATIVE SERVICES

Marc Linchuck
CEO

(301) 589-0088
(301) 589-6055 (fax)
MarcL@gispi.com

1700 Rockville Pike
Suite 230
Rockville, MD 20852

March 8, 2022

Re: Favor - **SB0639 - Consumer Protection – Security Questions and Measures**

Dear Maryland Legislators,

My name is Marc Linchuck, CEO of Global Investigative Services, Inc a Maryland based company in Montgomery County. My company has been in business since 1993 and in addition to being a licensed private investigation agency, we specialize in conducting pre-employment background checks, throughout the United States and parts of the world.

I personally have been involved with the company for the past twenty-three years learning all aspects of the background screening industry as well as investigations. Protecting consumer data and PII (Personally Identifiable Information) is incredibly important in our industry.

More than ever, our everyday lives are affected by the digital world around us. We sign user agreements, reset passwords, and answer security questions all without much thought. I am sure most of you have seen security questions like these on various websites claiming to keep our data safe: ***What was the name of your childhood friend? What street did you live on in the third grade? What was your childhood phone number?*** and the perennial favorite; **What is your Mother's Maiden Name?**

Over the past few years, we have seen companies like Home Depot, T-Mobile, Equifax and Facebook suffering from major data breaches. Although the initial breach is a concern, the information obtained by the hackers presents an ongoing risk. The information obtained can be used to access *other* accounts that may not have been subject to the original attack.

At this point in time, social media has become so ubiquitous that we don't even think about how much personal information we post in public online spaces. Facebook, having been open to all users since 2006, has nearly three billion users. Any "friend" could easily uncover the information they need to answer security questions discussed

above. It does not take an expert in computer forensics to uncover answers to the questions above.

Here is the perfect example:

A user shows a public connection to their mother. The mother, also a social media user, displays both her maiden and married names, which are visible to the public. With almost no effort, anyone with ill intentions now has that vital piece of information (mother's maiden name) and can potentially access data the original user thought was secure. Continuing to use that bit of PII as a security question or required piece of information to verify someone's identity is no longer rational.

I know there are many other examples I could mention, but I believe the one above makes the best point.

By prohibiting a business or a unit of State or local government from using the maiden name of the mother of a customer as a means of safeguarding access to the customer's account, would be a good step forward in preventing identity fraud and/ or something worse.

Thank you for the opportunity to share my view and I urge you to support SB0639.

Sincerely,

Marc Linchuck
CEO

SB0639_SponsorAmendment_283727-01
Uploaded by: Sen. Cheryl Kagan
Position: FAV

SB0639/283727/1

AMENDMENTS PREPARED BY THE DEPT. OF LEGISLATIVE SERVICES

09 MAR 22
10:31:59

BY: Senator Kagan
(To be offered in the Finance Committee)

AMENDMENTS TO SENATE BILL 639
(First Reading File Bill)

AMENDMENT NO. 1

On page 1, strike beginning with "Division" in line 8 down through "General" in line 9 and substitute "Department of Information Technology".

AMENDMENT NO. 2

On page 2, strike beginning with "**DIVISION**" in line 25 down through "**GENERAL**" in line 26 and substitute "**DEPARTMENT OF INFORMATION TECHNOLOGY**".

SB639_ Mother’s Maiden Name Expansion Testimony.pd
Uploaded by: Sen. Cheryl 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

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

SB639: Consumer Protection – Security Question Prohibition

Senate Finance Committee

Date: March 9, 2022 | 1pm

Last year, the Senate passed SB185 (46-0), which required financial institutions to provide an alternative to the security question "What is your mother's maiden name?" You may recall that during that hearing, I rattled off the maiden name of every Finance Committee member's mother. These names were easily found online through website searches using Ancestry.com, Newspapers.org, StateRecords.org, and even Facebook. In fact, a 2005 study effortlessly compiled the mother's maiden names (MMN) of 4,105,111 Texans using public records.

The MMN security question was created in 1882. This question no longer provides effective security 140 years later and offers data that allows our life savings to be easily hacked.

On a recent EHE Committee site visit to a Howard County school, I was asked for my MMN. Due to security concerns, I refused. Hacking is a very real threat, and cyberattacks are on the rise. In 2021, there were over 1,291 exposures of personal data, including Android (100+ million people); Facebook (553 million users); and LinkedIn (700 million/93% of users). IdentityForce found that businesses such as T-Mobile, CVS, and GEICO, have experienced data breaches in the past year.

On December 4, 2021, the MD Department of Health (MDH) was the victim of a malicious ransomware attack. If MDH had not shut down all of their services in a timely manner, hackers could have gotten access to Social Security numbers and other personally identifiable information. This would have allowed hackers to steal Marylanders' identities.

We must expand on last year's law applying to financial institutions in order to provide better protection. SB639 offers the logical next step by prohibiting businesses, as well as state and local government agencies, from using this dangerously outdated "security" question. Business enforcement would be handled by the Office of the Attorney General's Consumer Protection Division; an amendment would shift government responsibility to the Department of Information Technology.

I urge a favorable report on SB639.

SB639 - Maiden Name - CPD - Letter of Information.

Uploaded by: Steven M. Sakamoto-Wengel

Position: INFO

BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

Writer's Fax No.

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

Writer's Direct Dial No.
(410) 576-6307

March 9, 2022

TO: The Honorable Delores G. Kelley, Chair
Senate Finance Committee

FROM: Steven M. Sakamoto-Wengel
Consumer Protection Counsel for Regulation, Legislation and Policy

RE: Senate Bill 639 – Consumer Protection – Security Questions and Measures – LETTER OF INFORMATION

The Consumer Protection Division of the Office of the Attorney General hereby submits the following regarding Senate Bill 639, sponsored by Senator Kagan, which would prohibit a business or a unit of State or local government from using a person's mother's maiden name as a security measure to access an account. While a violation by a business would be a violation of Maryland's Consumer Protection Act, SB 639 provides that a person may report a violation by a unit of State or local government to the Consumer Protection Division.

Although the Division appreciates SB 639's intent of trying to protect Maryland citizens from identity theft by limiting the use of a security measure that isn't in-fact secure, reporting violations by governmental units to the Division would provide only an illusory remedy. The Division has no authority over State and local governmental units. While the Division mediates complaints against businesses, there is no precedent for mediating complaints against other governmental units. Although governmental units report data breaches to the Division, the purpose is so that the Division has the information it needs to provide consumers affected by the breach with assistance in protecting themselves. The Division has no authority to take enforcement or any other action against the governmental agency that experienced the data breach.

Accordingly the Consumer Protection Division respectfully requests that the Senate Finance Committee strike subsection (D), page 2, lines 24-26 when considering Senate Bill 639.

cc: Members, Senate Finance Committee
The Honorable Cheryl Kagan