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world of free information gathering across the Internet, requesting a person's mother's maiden name is flawed and outdated.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.