GLOBAL
INVESTIGATIVE SERVICES
Safe. Fast. Affordable.

HB274/ SB0160-FAVORABLE

Good Afternoon,

Chairperson Davis and members of the House Economic Matters 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 **HB274/ 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

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.