SB 0185/ HB0471- Favorable

Good Afternoon,

Chairperson Del. Derick Davis, and members of the House Economic Matters 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.