MD|DC
Credit Union Association

Chairman Dereck Davis
Room 231
House Office Building
Annapolis, Maryland 21401

HB117: Maryland Personal Information Protection Act – Revision
Testimony on Behalf of: MD|DC Credit Union Association
Position: Support

Chairman Davis, Vice-Chair Dumais, 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 respectfully support this bill.

Building trust by safeguarding consumers' money and personal information is the cornerstone of the credit union movement and the financial services industry. Consumers deserve to feel confident that their private information will not be compromised and that all entities in the payment ecosystem take this responsibility seriously. Unfortunately, we live in a time where data breaches are so prevalent, but we must do our due diligence to protect consumer information. Credit unions are member-owned, and we take the protection of our members very seriously.

I. This bill creates a uniform data protection standard for businesses and vendors who handle consumer data.

- **Data Protection Standards**
  - Our proposed language should not force any businesses or vendors to increase their current data security standards <u>if they are already following the existing industry standards to protect data.</u>

- **Private Cause of Action**
  - There should be shared responsibility for all those involved in the payment system for protecting consumer data. Credit unions' costs to replace cards and open new accounts for members who have, or may have, been breached are in the hundreds of millions of dollars. The state law should provide mechanisms to address the harms that result from privacy violations and security violations, including data breaches. Only the Attorney General (AG) can initiate a data breach-related lawsuit against a business in Maryland. The AG has no duty to act or to pay recovered funds to harmed financial institutions. This is unfair and unsustainable.

- **Small businesses are not the target**
  - In the years since we first brought this bill to the General Assembly, we have listened to all interested parties and have made significant changes to the language. We want to make it very clear that **<u>SMALL BUSINESSES ARE NOT THE TARGET</u>**. This bill only

MD|DC
Credit Union Association

pertains to businesses that employ over 250 people and have average annual gross receipts over $10 million in its most recently completed three fiscal years.

II. Financial institutions go to great lengths to protect data, and it is not fair that we must pay the price for the inaction of others.

Financial institutions are subject to the **Gramm-Leach-Bliley Safeguards Rule (GLBA).** To comply with this rule, financial institutions must develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature, scope of its activities, and the sensitivity of the customer information it handles. This plan must: **Designate** one or more employees to coordinate its information security program; **Identify** and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; **Design** and implement a safeguards program, and regularly monitor and test it; **Select** service providers that can maintain appropriate safeguards make sure their contract requires them to maintain safeguards, and oversee their handling of customer information; and **Evaluate** and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

III. Credit Unions, like all financial institutions, are supervised and examined regularly to ensure compliance with GLBA.

The safeguards rule is implemented and monitored by the National Credit Union Administration through NCUA Part 748, 12 CFR Appendix B to Part 748, and Chapter 6 of the NCUA Examiners Guide. During an examination, NCUA field staff focuses on proactive measures credit unions can take to protect their data and their members, including but not limited to:

- encrypting sensitive data
- developing a comprehensive information security policy
- performing due diligence over third parties that handle credit union data
- monitoring cybersecurity risk exposure
- monitoring transactions, and
- Testing security measures

If the examiner feels that any of these measures have not been adequately designed or implemented, they have many routes they can take to resolve the issue:

- Prompt corrective action order
- An Order to Cease and Desist, which requires a party to take action (or refrain from taking action), including making restitution
- An Order or Notice of Prohibition, which prohibits a party from ever working for a federally insured financial institution
- An Order Assessing Civil Money Penalties
- Documents of resolution
- Letters of understanding
- Agreement or consent order

MD|DC
Credit Union Association

IV. Many industries that handle sensitive consumer data are not subject to the strict government standards to which financial institutions must adhere.

The current framework in which financial institutions and hospitals implement strict data security measures to protect data, while many other businesses do not, is ineffective. Unless all entities that handle consumer data take steps to protect the data and are held accountable, we will not progress.

V. Data breaches have cost credit unions, banks, and the consumers they serve hundreds of millions of dollars, have compromised the consumers' privacy, and jeopardize their financial security. At the federal level, we have worked with the national banking trade associations on this type of legislation for years, with no movement from congress. (See Appendices A and B).

There have been tens of thousands of data breaches over the last two decades. When a business entity or vendor is breached, the first thing that many consumers do after notification is contact their financial institutions to see if their data is compromised. If the member wants to close their account, open a new one, and have their cards replaced, this costs the credit union both time and money. According to a Carnegie Mellon University published study, "estimates of the cost of reissuing cards range from $3 to $25 per card."[1] While costs widely vary, several data breaches have become infamous for their costs to financial institutions and demonstrate the scope of the problem.

1. The 2013 Target data breach costs "exceeded $200 million for financial institutions, according to data collected by the Consumer Bankers Association and the Credit Union National Association. The two trade associations said that 21.8 million of the 40 million compromised credit and debit cards have been replaced…and the cost to credit unions has increased to $30.6 million from an original estimate of $25 million."[2] Most notably, this class action lawsuit was filed in Minnesota, which has the **Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64, which is substantially similar to what we are asking for:**

> "Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:
> "(1) the cancellation or reissuance of any access device affected by the breach;
> (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;
> (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;
> (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and

[1] Graves, J. (2018). Should Payment Card Issuers Reissue Cards in Response to a Data Breach? Retrieved January 13, 2021, from https://www.andrew.cmu.edu/user/nicolasc/publications/Graves-WEIS14.pdf
[2] Target Data Breach Cost for Banks Tops $200M. (2015, June 11). Retrieved January 13, 2021, from https://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156

MD|DC
Credit Union Association

(5) the notification of cardholders affected by the breach"[3]

Following a lengthy class-action lawsuit brought by lenders in several states, Target settled and paid banks and credit unions about $20.25 million ($60 million to the class as a whole, of which approximately $17 million went towards lawyer fees).[4]

2. The Home Depot breach cost credit unions over 60 million dollars to reissue cards and cover other expenses. A credit union "industry survey on this breach found that 7.2 million credit union debit and credit cards were affected by the breach and that the cost of the violation per card issued by credit unions was $8.02 (which included costs for reissuing new cards, fraud, and all other expenses – such as additional staffing, member notification, account monitoring and others)."[5] The settlement from the Home Depot lawsuit was underwhelming. According to the settlement agreement, "Financial institutions that file a valid claim will be eligible to receive a fixed payment estimated to be $2.00 per compromised card without having to submit documentation of their losses and regardless of whether any compensation has already been received from another source; In addition, financial institutions that submit proof of losses are also eligible for a supplemental award of up to 60% of their documented, uncompensated losses from the data breach."

There have been thousands of other data breaches, and it is easy to see how the costs can quickly add up. As member-owned financial cooperatives with no external shareholder funding, this burden can be significant for credit unions. **The data protection standard should be clear and the remedy clearly defined.**

VI. Finally, the cost of a data breach to a company far outweighs the cost of taking the necessary precautions to protect data. As we move closer and closer to a fully tech-driven world of commerce, there is no reasonable excuse for not protecting consumer data.

As businesses ourselves, we never want to place an unnecessary burden on another company. However, in addition to the costs of a breach to innocent parties, the costs to a business itself are far more than the costs to protect data at the level required in this bill.

"After a data breach, businesses could face multiple types of financial detriment, which may include:

-
- Merchant processor compromise fines: $5,000 – $50,000
- Forensic investigation: $12,000 – $100,000+
- Onsite QSA assessments following the breach: $20,000 – $100,000
- Free credit monitoring for affected individuals: $10-$30/card
- Card re-issuance penalties: $3 – $10 per card

[3] 325E.64 Access Devices: Breach of Security
[4] In re Target Corp., MDL No. 14-2522 (PAM)
[5] Association, C. (2018, June 30). Home Depot Data Breach Cost Credit Unions Nearly $60 Million. Retrieved January 13, 2021, from https://www.prnewswire.com/news-releases/home-depot-data-breach-cost-credit-unions-nearly-60-million-280973342.html

MD|DC
Credit Union Association

- Breach notification costs: $2,000 – $5,000
- Technology repairs: $2,000 - $10,000
- Increased in monthly card processing fees
- Legal fees, and Civil judgments"[6]

"If you're a small business, PCI DSS compliance should cost from $300 per year (depending on your environment)**...**If you're a very large enterprise and need a PCI DSS assessment, expect to pay $70,000+ in total costs (depending on your environment)."[7]

If we continue to "kick the can down the road," we are only delaying the inevitable. Unfortunately for consumers and businesses like credit unions, we will continue to pay the price until action is taken.

As always, we appreciate the ability to have our voices heard and look forward to a continued partnership. 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

[6] https://www.securitymetrics.com/blog/how-much-does-data-breach-cost-your-organization
[7] Id.

MD|DC
Credit Union Association

Appendix A (Excerpts from Congressional Comment Letter)

ICBA
Independent Community Bankers of America®

Privacy Rights and Data Collection: The Community Bank Perspective

Chairman Crapo, Ranking Member Brown, members of the Committee, the Independent Community Bankers of America, representing community banks across the nation with more than 52,000 locations, appreciates the opportunity to provide this statement for the record in connection with today's hearing on "Privacy Rights and Data Collection in a Digital Economy." ICBA greatly appreciates your opening the discussion of a critical public policy issue that will only become more significant as the digital economy becomes more pervasive.

Community banks are committed to safeguarding consumer data and honoring consumers' preferences in the use of such data. Attached is a comprehensive statement of community banks' policies, practices, and preferences with regard to the collection and use of personally identifiable information ("PII"), which was previously submitted to this committee in response to your request. Below we highlight the principles which will guide our evaluation of any proposed legislation in this area:

- ICBA supports current privacy standards, such as those in the Gramm-Leach-Bliley Act ("GLBA"). To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions.
- A national breach notification standard would be a good first step to ensure consistent consumer notification in the case of a breach, rather than a patchwork of state laws in this area.
- ICBA supports the current privacy notice requirements. Banks are required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.
- Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information.
- Third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Guidelines"), implementing the Gramm-Leach-Bliley Act.
- The credit reporting agencies ("CRAs"), also known as credit bureaus, should be subject to comparable supervision and examination as banks.
- CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.
- Non-bank entities accessing customer account data must be held responsible for ensuring the security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause.
- Consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

By their very nature, community banks and other financial institutions must collect sensitive nonpublic personally-identifiable information ("PII")[4] about customers to meet their needs for financial services, which includes an array of deposit and loan services. This information is also used to prevent fraud, identity theft and comply with various regulatory requirements. Safeguarding customer information is central to financial institutions maintaining public trust and retaining customers.

[2] 12 C.F.R. Part 30, Appendix B. and The Financial Modernization Act of 1999, the "Gramm-Leach-Bliley Act," P.L. 106-102.

[3] The Financial Modernization Act of 1999, the "Gramm-Leach-Bliley Act," P.L. 106-102. The "Interagency Guidelines Establishing Information Security," 12 C.F.R. Part 30, Appendix B. FFIEC IT Examination Handbook, https://ithandbook.ffiec.gov/.

[4] Nonpublic personal information is a term commonly referenced in regulations. Nonpublic personal information is, generally speaking, personally identifiable financial information that is not publicly available. It is also defined as information that is not publicly available and that:

- a consumer provides to a financial institution to obtain a financial product or service from the institution;
- results from the transaction between the consumer and the institution involving service; or a financial product or
- a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

ICBA has consistently advocated that all participants in the payments and financial systems, including merchants, aggregators and other entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards. Similarly, any entity that processes or holds personally sensitive information about consumers should be required to safeguard that information, just as banks are required. Under current federal law, retailers and other parties that process or store sensitive consumer information are not subject to the same federal data security standards and oversight as financial institutions. Securing personally sensitive data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing and collecting points. To most effectively secure customer data and thereby protect consumer privacy, all entities that store or process sensitive personal information, and all entities with access to customer financial information, should be subject to and maintain well-recognized standards such those in the Gramm-LeachBliley Act and implementing regulations.

Below is a general overview of some of the legal and regulatory requirements to which banks are subject, and for which they are examined and supervised. These requirements include, but are not limited to, the Gramm-Leach-Bliley Act, the "Interagency Guidelines Establishing Information Security," and the Federal Financial Institutions Examination Council's IT

MD|DC
Credit Union Association

As community-based institutions, a community bank's success is in large part dependent on its reputation. Maintaining the integrity of customer accounts is of utmost importance to community banks, not only because it is required by law, but also because it is the right thing to do. If a customer experiences an adverse event which results in financial loss caused by a breach or failure by a permissioned third party, it is likely that customer will look to his or her bank with the expectation of being made whole. When a loss occurs through no fault of a community bank, but because of the failing of a third party, that third party should be held responsible. For example, there should be certainty as to whether consumers would be protected under the Electronic Fund Transfer Act for unauthorized debits when consumers share their account information.

Furthermore, community banks have a vital stake in containing any damage caused by hackers, identity thieves and breaches to third parties. Regardless of where a breach occurs, banks are the stewards of the customer financial relationship. They take measures to restore consumer confidence in the financial system and absorb any upfront costs, which may be significant, of third-party intrusions by responding to customer concerns and inquiries, protecting against fraud and absorbing other expenses. Therefore, any costs associated with a breach or hack should be borne by the entity that incurs the breach. Firms with third-party access to a consumer's account should bear full liability for any consumer harm resulting from a breach to its system.

ICBA appreciates the opportunity to provide our views on these questions. We welcome a further discussion with the Committee on these and other related topics. Should you have any questions, please reach out to Jeremy Dalpiaz of my staff by email at Jeremy.Dalpiaz@icba.org or by phone, 800-422-8439.

Sincerely,

Rebeca Romero Rainey
President and CEO

8975 Guilford Road, Suite 190, Columbia, MD 21046
P 800-492-4206 F 410-290-7832
E info@mddccua.org
mddccua.org

MD|DC
Credit Union Association

Appendix B (Excerpts from Congressional Comment Letter)

American Bankers Association
Building Success. Together.

James Ballentine
Executive Vice President
Congressional Relations
And Political Affairs
202-663-5359
jballent@aba.com

March 15, 2019

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing
and Urban Affairs
U.S. Senate
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing
and Urban Affairs
U.S. Senate
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

For ABA members, regardless of the commercial or government entity involved, it is vital that privacy legislation requires all entities handling sensitive personal information implement and maintain adequate security measures to protect that information and provide notice to individuals who are subjected to harm resulting from a breach of their information.

It is important that any privacy legislation containing a national standard must provide robust, exclusive enforcement of this national standard by the appropriate federal or state regulators across all industry sectors. This must include preserving GLBA's existing administrative enforcement structure for financial institutions, including banks.

*Note: ABA has not voiced support for a private right of action for financial institutions