Testimony of

Wm. Douglas Johnson

On behalf of the

American Bankers Association

before the

Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

of the

Committee on Commerce, Science, and Transportation

United States Senate

Testimony of
Wm. Douglas Johnson
On behalf of the
American Bankers Association
before the
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
of the
Committee on Commerce, Science, and Transportation
United States Senate

Thursday, February 5, 2015

Chairman Moran, Ranking Member Blumenthal, my name is Doug Johnson, Senior Vice President, payments and cybersecurity policy, of the American Bankers Association. In that capacity, I currently lead the association's physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership. I appreciate the opportunity to be here to represent the ABA and discuss the importance of instituting a uniform federal data breach law in place of disparate state laws. The ABA is the voice of the nation's $15 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $11 trillion in deposits and extend over $8 trillion in loans.

As the 114th Congress engages in public debate on the important issue of data security, we share your concerns about protecting consumers in this increasingly sophisticated world of electronic commerce and record keeping. It is clear that consumers enjoy the efficiency and convenience of conducting transactions electronically. Notwithstanding these recent breaches, our payment system remains strong and functional. No security breach seems to stop the $3 trillion that Americans spend safely and securely each year with their credit and debit cards. And with good reason: Customers can use these cards confidently because their banks protect them from losses by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs. While the vast majority of these transactions are conducted safely,

occasional breaches will continue to occur. Consumers have a right to swift, accurate, and effective notification of such breaches. They also have a right to trust that, wherever they transact business electronically, the business is doing everything it can to prevent that breach from occurring in the first place.

The banking industry supports effective cyber security policy and will continue to work with Congress to achieve that goal. Banks are acknowledged leaders in defending against cyber threats. Therefore, from the financial services perspective it is critical that legislation takes a balanced approach that builds upon – but does not duplicate or undermine – what is already in place and highly effective in the financial sector.

In my testimony I will focus on three main points:

- **The value of a national data breach standard.** Consumers' electronic payments are not confined by borders between states. As such, a national standard for data security and breach notification is of paramount importance.
- **The importance of recognizing existing Federal breach requirements.** Any Federal data protection and notification requirement must recognize existing national data protection and notification requirements.
- **The need for strong national data protection requirements.** All parties must share the responsibility, and the costs, for protecting consumers. The costs of a data breach should ultimately be borne by the entity that incurs the breach. To limit such breaches, any comprehensive data breach requirement must have strong data protection requirements applicable to any party with access to important consumer financial information.

I. The Value of a National Data Breach Standard

Our existing national payments system serves hundreds of millions of consumers, retailers, banks, and the economy well. It only stands to reason that such a system functions most effectively when it is governed by a consistent national data breach policy.

Currently, 46 states, three U.S. territories, and the District of Columbia have enacted laws governing data security in some fashion, such as standards for data breach notification and for the safeguarding of consumer information. Although some of these laws are similar, many have

inconsistent and conflicting standards, forcing businesses to comply with multiple regulations and leaving many consumers without proper recourse and protection. Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification requirements. In the event of a breach, the public should be informed where it occurred as soon as reasonably possible to allow consumers to protect themselves from fraud.

Given the mobile nature of our nation's citizens, it is clear that the existing patchwork of state data breach laws are unduly complicated for consumers as well as businesses. For instance, consider a couple residing in a northern state who winter in a southern one and have their credit card data compromised at a merchant in a third state. In this instance, the couple wants to be alerted that their financial data has been compromised and that they are protected. Determining where the couple may or may not reside and which state laws may or may not apply unduly complicates the simple need to protect the couple from financial harm. It also diverts resources at the merchant and the bank toward determining how to comply with a myriad of laws as opposed to fixing the problem.

We believe that the following set of principles should serve as a guide when drafting legislation to provide stronger protection for consumer financial information:

1. Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification standards.
2. Strong national data protection and consumer notification standards with effective enforcement provisions must be part of any comprehensive data security regime, applicable to any party with access to important consumer financial information.
3. Requirements for industries that are already subject to robust data protection and notification requirements must be recognized.
4. In the event of a breach, the public should be informed where it occurred as soon as reasonably possible to allow consumers to protect themselves from fraud. The business with the most direct financial relationship with affected consumers should be able to inform their customers and members about information regarding the breach, including the entity at which the breach occurred.
5. The costs of a data breach should ultimately be borne by the entity that incurs the breach.

II. The Importance of Recognizing Existing Federal Breach Requirements

As we enact a national data breach requirement, some industries – including the financial industry – are already required by law to develop and maintain robust internal protections to combat and address criminal attacks, and are required to protect consumer financial information and notify consumers when a breach occurs within their systems that will put their customers at risk.

Title V of the Gramm-Leach-Bliley Act (GLBA) requires banks to implement a "risk-based" response program to address instances of unauthorized access to customer information systems. At a minimum, a response program must:

1. Assess the nature and scope of any security incident and identify what customer information systems and customer information may have been accessed or misused;
2. Notify the institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information."
3. Notify appropriate law enforcement authorities and file Suspicious Activity Reports in situations involving federal criminal violations requiring immediate attention;
4. Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information, and
5. Notify customers "as soon as possible" if it is determined that misuse of customer information has occurred or is reasonably possible.

A critical component of the GLBA guidelines is customer notification. When a covered financial institution becomes aware of a material breach of "sensitive customer information," it must conduct a reasonable investigation to determine whether the information has been or can be misused. If it determines that misuse of the information "has occurred or is reasonably possible," it must notify affected customers "as soon as possible."

Under GLBA, sensitive customer information includes the customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, credit card, debit card or other account number or personal identification number.

Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password.

A covered financial institution must also provide a clear and conspicuous notice. The notice must describe the incident in general terms and the type of customer information affected. It must also generally describe the institution's actions to protect the information from further unauthorized access and include a telephone number. The notice also must remind customers to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution.

Where appropriate, the notice also must include:

1. Recommendation to review account statements immediately and report suspicious activity;
2. Description of fraud alerts and how to place them;
3. Recommendation that the customer periodically obtain credit reports and have fraudulent information removed;
4. Explanation of how to receive a free credit report; and
5. Information about the FTC's identity theft guidance for consumers.

We believe the extensive breach reporting requirements currently in place for banks provide an effective basis for any national data breach reporting requirement for businesses generally.

III. The Need for Strong National Data Protection Requirements

Any legislation focused on creating a national standard for breach notification should also include a complementary national data security standard for covered entities. If Congress does not address data security standards now it misses the opportunity to instil a greater overall level of data security protections for consumers.

Every business must share in the responsibility to protect consumers. With that responsibility should come the requirement for that business, whether it be a bank, merchant, third party processor or other entity, to bear the costs for any breach they incur.

To limit the potential for data breaches in the first place, any comprehensive national data breach requirement should be enacted in tandem with strong data protection requirements applicable to any party with access to important consumer financial information. Limiting the potential for such breaches through strong data protection is the first, essential, line of defense in our efforts to maintain customer trust and confidence in the payments system

Effective data protection requirements are scalable. For instance, bank regulations, through GLBA, recognize that the level of risk to customer data varies significantly across banks. Large banks require continual, on-site examination personnel, while community-based institutions are subject to periodic information security examinations.

Data security is also an ongoing process as opposed to the state or condition of controls at a point in time. As opposed to proscribing specific technological security requirements, GLBA and the associated bank regulatory requirements are risk and governance-based. Bank security programs are required to have "strong board and senior management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities."[1]

IV. The Path Forward

The legal, regulatory, examination and enforcement regime regarding banks ensures that banks robustly protect American's personal financial information. We believe that this regime provides an appropriate, scalable model for other businesses entrusted with sensitive customer financial and other information.

[1] Federal Financial Institution Examination Council IT Handbook, available at http://ithandbook.ffiec.gov/it-booklets/information-security/introduction/overview.aspx