April 30, 2015

Honorable Members of Congress:

The severity and intensity of data security breaches has risen dramatically in recent years and cannot be denied. American consumers and businesses have been the victims of rampant data theft as a result of high-profile cyber-attacks on major financial institutions, large retailers, health care companies, and even the entertainment industry. As a result, hundreds of millions of Americans' sensitive personal and financial information has been compromised.

We applaud Congressional efforts to improve public and private cybersecurity measures, and the bipartisan approach to strengthening cyber security protections, improving information sharing, and enhancing consumer notification standards in the event of a breach. But despite these efforts, a gaping vulnerability in data security will remain if credit card security is not addressed.

While the use of electronic and mobile payment methods has grown, traditional credit and debit cards still account for two-thirds of all purchases by value in the United States. Moreover, since payment processes are connected to expansive networks and data centers, ensuring their security at the point-of-sale must be an utmost priority. As such, we feel Congress must urge the nation's largest credit card issuers – particularly the big banks and credit unions – to do everything they can to provide the best possible safeguards to protect consumers and their financial transactions.

The best way to keep consumer data safe is the implementation of chip and PIN credit card technology. While many card issuers are increasingly deploying new chip-enabled cards that encrypt data at point-of-sale terminals during transactions, those cards unfortunately still rely on a signature as a secondary form of verification – a system that provides little to no added protection. Signature verification is not a credible element of security as it can be easily forged or altogether ignored.

Instead, chip-enabled cards must be coupled with the requirement that consumers enter a personal identification number (PIN) to properly authorize a transaction. The PIN requirement adds a distinct layer of security and complexity to each transaction that dramatically reduces fraud.

Evidence of chip and PIN's benefits and heightened security protections were highlighted in President Obama's Executive Order – issued last October – that required chip and PIN technology for government issued credit cards and an upgrade of point-of-sale terminals at federal buildings. It was an important step, but more must be done to expand these protections for *all* Americans.

Only the dual chip and PIN combination provides Americans the safeguards they deserve. In fact, chip and PIN cards have long been the standard in many European countries where they have experienced a sharp decline in counterfeit and fraudulent transactions since the cards were implemented.

While chip and PIN cards are not a cure-all for every instance of fraud or theft, they are an important element of safeguarding the transactions that millions of Americans make every day. So as you continue your work on cyber and data security legislation, we urge you to be mindful of this important consumer protection issue and support broad adoption of chip and PIN credit card technology – the best payment security technology available today to protect American consumers.

Thank you for considering our views. We look forward to working together on this critical issue.

Sincerely,

Debra Berlyn
Organizer of ProtectMyData.org

Kim Keenan
CEO of the Multicultural Media, Telecom and Internet Council (MMTC)

Rosa Mendoza
Executive Director of the Hispanic Technology and Telecommunications Partnership (HTTP)

Jeremy White
Founder of DiverseTech

CC: The Honorable Barack Obama, President of the United States
The Honorable Janet Yellen, Chair of the Federal Reserve
The Honorable Richard Cordray, Director of the Consumer Financial Protection Bureau