



January 21, 2014

The Honorable John Boehner
Speaker of the House of Representatives
Washington, D.C. 20515

The Honorable Harry Reid
United States Senate
Washington, D.C. 20510

Dear Mr. Speaker and Senator Reid:

At the end of last year, a sophisticated criminal attack to steal proprietary customer financial data and other customer information was perpetrated against Target Corporation, Neiman Marcus, and several other retailers. Among other things, this series of cyber attacks raises questions about the security of the basic payment systems utilized in the United States and has reignited a public debate about data theft and the security of information. The National Retail Federation and our 12,000 members are committed to combating this criminal threat to our industry and our customers, and we strongly recommend the adoption of meaningful steps to fight cyber theft and credit card fraud.

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy.

Many of the details about the scope and breadth of the data theft involving retailers remain unknown as a result of the ongoing investigation by the United States Secret Service (USSS). A report released last Thursday by the USSS, US-CERT, and iSight Partners of Dallas indicates the malware used in this attack was elaborate and required a high degree of skill in executing the attack. The report provides a glimpse into a world of highly motivated criminals using state of the art tools with the capability of attacking not only retailers, but also other American businesses, financial services companies, and even the U.S. government.

When it comes to the most criminally lucrative data—sensitive bank card information—our partners in the financial sector have a critical role to play in making sure their cards are secure. For years, banks have continued to issue fraud-prone magnetic stripe cards to U.S. customers, putting sensitive financial information at risk while simultaneously touting the security benefits of next generation “PIN and Chip” card technology for customers in Europe and dozens of other markets.

The retail industry is eager to work with banks and card companies to fight cyber attacks and reduce fraud. In fact, several large retailers have been trying to lead in the payment security space through the adoption of new technology. These efforts include installation of sophisticated new PIN-enabled point of sale (POS) systems and readiness to adopt cards with more secure microchip technology, but the fact remains that retailers cannot do this alone. Only by working together will consumers' financial data be protected from criminals. That is why it is time for our partners in the card industry to invest in next generation technology to secure sensitive bank card data. Adopting “PIN and Chip”

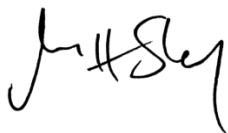
security measures in the U.S. (as the branded card networks and issuing banks have done to protect European consumers) would be a good start. As long as bank cards continue to be issued with outdated and fraud-prone magnetic stripe (and signature) security, it is clear American card holders will remain largely unprotected.

As this discussion moves forward, NRF would like to reiterate our support for the following policy initiatives:

- **“PIN and Chip” payment card security** – The most secure payment card available has both an electronic chip in the card and requires use of a PIN number for credit transactions (not just debit transactions), which is currently a payment card security standard widely used in Europe. Unlike signatures, PINs can be encrypted, so that even if the card data is acquired by a hacker, the encrypted PIN serves as an additional layer of security to help protect consumers. While criminal hacking incursions in the U.S. have been increasing in recent years, the U.K. Card Association reports that adoption of next generation technology has helped reduce fraud in the U.K. by more than 70% over the same period of time. If U.S. banks lead the adoption of universal PIN and Chip cards for American consumers, we will see a striking reduction in the incidence of fraud here as well.
- **Federal cybersecurity law** – NRF supports the passage by Congress of the bipartisan “Cyber Intelligence Sharing and Protection Act” (H.R. 624) so that the commercial sector can quickly share information about threats, as well as legislation that provides support for law enforcement to ensure that these crimes are thoroughly investigated and prosecuted.
- **One uniform Federal breach notification law** – For nearly a decade, NRF has supported passage of a single, nationwide standard for breach notification that would be modeled on, and preempt, the varying breach notification laws currently in operation in 46 states and the District of Columbia. A preemptive federal breach notification law would allow retailers to focus their resources on complying with one single law and enable consumers to know their rights, regardless of where they live.

Credit card fraud cost retailers and our financial services partners more than \$11 billion in 2012. That is why NRF is committed to a long-term solution to the issue, working with all stakeholders to ensure that our customers’ sensitive information is protected.

Sincerely,



Matthew R. Shay
President & CEO
National Retail Federation

cc: Members of the United States Senate
Members of the United States House of Representatives