To: All Attorneys General
Chief Deputies
Executive Assistants
Consumer Protection Contacts

From: Attorney General George Jepsen, Connecticut
Attorney General Sam Olens, Georgia

Re: **Sign-on Letter Urging Expedited Implementation of Chip and PIN Technology**

Date: October 14, 2015

DEADLINE FOR RESPONSE: WEDNESDAY, OCTOBER 28, 2015 at 12:00 PM (EST)

Enclosed please find a draft sign-on letter to be sent to major card brands and issuers, urging them to expedite the implementation of chip and PIN technology in the United States. Put simply, and as set forth in the letter, we strongly believe that chip and PIN should be the standard here just as it is in many countries around the world, and without any further unnecessary delay.

As we all know too well, in recent months, millions of U.S. consumers have been impacted by security incidents compromising their personal information, including massive, unprecedented breaches at major retailers. As Attorneys General, we are at the front lines of investigating those breaches and helping harmed consumers. The unfortunate reality is that as hackers become more sophisticated, consumers and businesses will continue to be impacted by data breaches for the foreseeable future. For this reason, payment card security and fraud prevention are more important than ever.

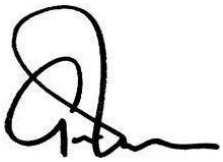
In our letter, we point out that as card issuers, banks and credit card companies share in the responsibility for protecting the personal and financial information of their customers. As it currently stands, however, most chip cards being issued in the United States rely on a signature, rather than a PIN, as the secondary form of verification. In our view, this is a less secure standard, since signatures can easily be forged or copied or even ignored at the point-of-sale.

The letter stresses that, in order to better protect consumers, chip-enabled cards issued in this country should be reinforced with the requirement that consumers enter a PIN to verify the transaction. Unlike signatures, PIN numbers can be changed easily and as frequently as needed by the consumer. Absent this additional protection, our citizens will be more vulnerable to damaging data breaches.

The letter highlights that chip and PIN technology is already widely used throughout Europe and other regions with great success, and many countries have since reported significant reductions in fraud. By contrast, studies indicate that the United States has been disproportionately affected by fraud in recent years. Further, in the wake of recent data breaches, information has come to light indicating that credit and debit cards in this country were more valuable on the black market because these cards lacked chip technology. If we continue to settle for weaker standards here, we will continue to pay the price.

Please return the attached response form to Allie McGuire at NAAG either via facsimile to (202) 521-4052 or via email in PDF form to amcguire@naag.org no later than noon eastern on Wednesday, October 28, 2015. Please contact Assistant Attorneys General Matthew Fitzsimmons or Michele Lucan from the Connecticut Attorney General's Office at (860)808-5440 or matthew.fitzsimmons@ct.gov and Michele.lucan@ct.gov, or Timothy Butler, Counsel for Legal Policy & Deputy Solicitor General for the Georgia Attorney General's Office at (404)651-9365 or tbutler@law.ga.gov with any substantive questions about the letter.

Sincerely,



George Jepsen
Connecticut Attorney General

Sam Olens
Georgia Attorney General

DRAFT LETTER

October 28, 2015

Walter M. Macnee, Vice Chairman
Ajaypal S. Banga, President/CEO
MasterCard, Inc.
2000 Purchase Street
Purchase, NY 10577-2509

Charlie Scharf, Chief Executive Officer
Visa, Inc.
900 Metro Center Blvd
Foster City, CA 94404

David W. Nelms, Chairman/CEO
Discover Financial Services
2500 Lake Cook Road
Riverwoods, IL 60015

Brian T. Moynihan,
Chairman/President/CEO
Bank of America Corp.
Bank of America Corp Center
100 North Tryon Street
Charlotte, NC 28255

Richard Dana Fairbank,
Chairman/President/CEO
Capital One Financial Corp.
1680 Capital One Drive 12th Floor
Mclean, VA 22102-3491

Michael Corbat, Chief Executive Officer
Citigroup Inc.
399 Park Avenue
New York, NY 10043

Kenneth I. Chenault, Chairman/CEO
American Express Co.
World Financial Center
200 Vesey Street
New York, NY 10285

James Dimon, Chairman/President/CEO
JPMorgan Chase & Co
270 Park Avenue
New York, NY 10017

Dear Sirs:

As state Attorneys General, we have a strong interest in ensuring that the personal and financial information of our citizens is safeguarded from fraud and unauthorized disclosure, and that the best possible protections against such misconduct are employed by the institutions and companies doing business in our states and nationwide. To this end, we write to urge you to expedite the implementation of chip and PIN technology in the United States. This technology is neither new nor novel. To the contrary, it is already widely used throughout Europe and other regions with great success. American consumers and businesses deserve no less. It is concerning that you have not acted more quickly to implement an obvious, effective and available consumer protection measure.

As you are well aware, consumers have come to rely on credit and debit card payment transactions with more and more frequency.[1] Along with this increasing reliance on card transactions, came a proliferation of data breaches[2] and a surge in fraudulent transactions.[3] As Attorneys General, we are at the front lines of investigating those breaches. In recent months, tens of millions of consumers in this country have been impacted by security incidents compromising their personal information, including massive, unprecedented breaches at major retailers.[4] American businesses are also affected, of course, bearing many millions of dollars in costs due to fraudulent transactions. Time and again, attackers have targeted payment systems and private financial information,[5] seemingly exploiting our continued reliance on outdated and less secure magnetic-stripe payment cards.[6]

For example, in Connecticut alone, approximately 515 data breach notifications were received last fiscal year—or, about 42 per month.[7] In total, around 2.5 million Connecticut residents are reported to have been affected by these breaches with varying categories of personal information implicated.[8] Significantly, nearly half of the reported breaches involving Connecticut residents— 235 breaches— involved compromised credit and debit card information.

The cost and inconvenience to consumers involved with the theft of financial information cannot be overstated. According to research, "individuals whose credit or debit cards were breached in the past year were nearly three times more likely to be an identity fraud victim."[9] Also telling, of the 350,000 cards potentially exposed in a recent retail breach, 9,200 cards are known to have been used fraudulently.[10]

---

[1] *See* "2013 Federal Reserve Payments Study: Recent and Long-Term Payment Trends in the United States: 2003 – 2012" (hereinafter, "2013 Federal Reserve Payments Study"), Federal Reserve System, December 19, 2013, p. 6-8.

[2] According to the Privacy Rights Clearinghouse, more than 884 million records have been involved in data breaches since 2005. See http://www.privacyrights.org/data-breach (last checked October 13, 2005).

[3] *See* "The EMV Chip Card Transition: Background, Status, and Issues for Congress," (hereinafter, "EMV Chip Card Transition Report") Congressional Research Service, September 8, 2015, p. 3 ("Between 2004 and 2010, fraud committed on U.S.-issued bank credit cards rose 70%"); 2013 Federal Reserve Payments Study, p. 6 (In 2012, the overall number of unauthorized transactions was estimated at 31.1 million, with a value of 6.1 billion).

[4] For example, the recent cyber-attack at Target put payment card information at risk for approximately 40 million credit and debit cards, while the Home Depot breach is estimated to have compromised 56 million payment cards. See "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," December 19, 2013, http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores and "The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores," September 18, 2014, http://media.corporate-ir.net/media_files/IROL/63/63646/HD_Data_Update_II_9-18-14.pdf

[5] *See* 2015 Verizon Data Breach Investigations Report, p. 5 ("[RAM-scraping] malware was present in some of the most high-profile retail data breaches of the year, and several new families of RAM scrapers aimed at point-of-sale (POS) systems were discovered in 2014."), p. 32 (POS intrusions accounted for 28.5 percent of confirmed data breaches reported for 2014).

[6] *See* EMV Chip Card Transition Report, p. 5 ("POS intrusions and the ensuing card fraud are facilitated by what many consider to be the weak link in the U.S. card payment process: the continued use of magnetic stripe cards that carry unencrypted data").

[7] Connecticut Office of the Attorney General Annual Report, Fiscal Year 2014-2015, p. 22 http://www.ct.gov/ag/lib/ag/about_us/annualreport2014-15.pdf.

[8] *Id*.

[9] Javelin Strategy & Research, March 2, 2015, https://www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/.

[10] *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015).

While federal law limits consumer liability for unauthorized charges, these protections are not all encompassing, and unless consumers are extremely vigilant, they could face serious financial harm.[11] At the very least, victims face the hassle of rectifying fraudulent charges, cancelling their cards and/ or changing account information, and waiting for new cards to be delivered. For the banks and companies shouldering many of the direct financial losses, the costs are dramatic, especially when combined with potential consequences like reputational harm and loss of consumer trust. As losses of credit card fraud are shifted to retailers, businesses in our states are at risk of similarly significant and mounting financial harms.

The unfortunate reality is that as hackers become more and more sophisticated, our consumers and businesses will continue to be impacted by data breaches for the foreseeable future. For this reason, payment card security and fraud prevention are more important than ever.

As the leading card brands and issuers of credit cards, you share in the responsibility for protecting the personal and financial information of their customers. Implementation of chip-enabled cards in the United States is imperative in order to provide stronger payment security and assurance to consumers. As it currently stands, however, most chip cards being issued in the United States rely on a signature, rather than a PIN, as the secondary form of verification.[12] There can be no doubt that this is a less secure standard, since signatures can easily be forged or copied or even ignored at the point-of-sale.[13]

In order to better protect consumers, the chip-enabled cards issued in this country must be reinforced with the requirement that consumers enter a PIN to verify the transaction. Unlike signatures, PIN numbers can be changed easily and as frequently as needed by the consumer. Absent this additional protection, your customers and our citizens will be more vulnerable to damaging data breaches. This is something we cannot accept, and nor should you.

As stated above, chip and PIN technology is nothing new. By the end of 2012, there were 1.62 billion chip cards in use across 80 countries around the world.[14] The chip and PIN approach is considered by many to be the gold standard currently for payment card security.

---

[11] Under the Electronic Fund Transfer Act, 15 USC § 1693 *et seq*., and Federal Reserve Regulation E, 12 CFR § 205 *et seq*., consumer liability for fraudulent ATM or debit card transactions depends on how quickly it is reported by the consumer. For example, if not reported within two business days after discovering the loss or theft, consumers could be held liable for up to $500. If reported more than 60 days after the statement listing the unauthorized withdrawals is sent, the consumer could be liable for all funds taken from the account, and possibly more (i.e. money in accounts linked to the debit account). 12 CFR § 205.6(b)(2) and (3).

[12] *See* "Chip Credit Cards: EMV, Chip and PIN, and Chip and Signature," https://www.creditcardinsider.com/learn/chip-and-signature-chip-and-pin-emv-cards/.

[13] *See* "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud," Federal Reserve Bank of Kansas City, Richard J. Sullivan, First Quarter 2013, p. 61 ("Fraud types and rates of success differ for card payments authorized by signature and those authorized by personal identification number (PIN). Because forging signatures is easier than stealing PINs, the loss per dollar for signature-authorized payments is significantly higher than losses for PIN payments.")

[14] EMV Chip Card Transition Report, p. 1 (citing "Continued Market Adoption of EMV Technology," EMVCo Newsletter, May 2013, http://www.emvco.com/newsletters/2013-May.html#section2).

Based on reports, countries that have implemented chip and PIN cards have seen significant reductions in fraudulent transactions.[15]

If employed here in the United States, PIN-based verification is likely to reduce fraud as is it has done in other places.[16] Some have claimed that chip and PIN technology will be burdensome or confusing to consumers. We believe any burdens will be minimal and justified by the dramatic security improvements offered by this technology. Many American consumers are already accustomed to using PINs in financial transactions, including those involving debit cards.[17] Furthermore, a poll conducted in November 2014 indicated that American cardholders are supportive of chip and PIN technology.[18]

Since 2003, the U.S. has consistently accounted for about half of the global loss from fraudulent transactions, despite that it is responsible for only a quarter of total card payments.[19] In the wake of recent wide-scale data breaches, information came to light indicating that credit and debit cards issued in this country were more valuable on the black market because these cards lacked chip technology.[20] We must not continue to pay the price for settling for weaker standards.

Put simply, chip and PIN technology should be implemented in the United States just as it is in many countries around the world, and without any further unnecessary delay. Payment system participants must commit to offering the greatest amount of protection and assurance to American consumers and businesses. Again, we urge you to step up to the plate and expedite the implementation of this more secure technology. To the extent you are requiring chip and PIN for all cards now, or have plans to do so in the immediate future, we would welcome the opportunity to discuss with you.

---

[15] *See* http://www.smartcardalliance.org/wp-content/uploads/EMV-FAQ-update-April-2015.pdf (Since transitioning to chip and PIN, the U.K. reported that retail fraud fell by 67 percent and lost and stolen card fraud fell by 58 percent between 2004 and 2009; in Canada, after its roll-out of EMV in 2008, losses from debit card skimming fell from CAD$142 million in 2009 to CAD$38.5 million in 2012); EMV Chip Card Transition Report, p. 16 (on the other hand, we lack information about the impact of chip and signature cards on fraud reduction because this method has not been adopted in other countries).

[16] *See Id*.; *see* also "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud," Federal Reserve Bank of Kansas City, Richard J. Sullivan, First Quarter 2013, p. 74 ("If the use of EMV payment cards in the [U.S.] leads to a fraud loss pattern similar to the patterns seen in France, the Netherlands, and the UK, then U.S. fraud losses could fall by as much as 40 percent."). Alarmingly, if U.S. issuers continue to allow signature verification for chip transactions, fraud could rise. *Id*. p. 74-75 ("Many countries that use EMV payment cards do not allow cardholder authentication with signatures. Issuers in the United States, however, appear likely to continue to allow signature authorization on EMV debit and credit card transactions. As a result, fraud on lost or stolen cards may not decline in the [U.S.]. Fraud may even rise as fraudsters, unable to commit fraud on counterfeit cards, begin to target payments with relatively weak security, such as transactions that allow signature authorization").

[17] 2013 Federal Reserve Payments Study, p. 8 ("The number of debit card payments exceeded the number of credit card payments for the first time in 2004. By 2012, the number of debit card payments had reached 47 billion—much higher than the 26.2 billion credit card payments in the same year").

[18] *See* http://www.chipandpinsecuritynow.org/about/ (reporting that 82% of consumers support chip and PIN, and that 52% would consider changing banks for this security).

[19] EMV Chip Card Transition Report, p. 2-3 (citing "Skimming off the Top: Why America Has Such a High Rate of Payment-Card Fraud," Economist.com, February 15, 2014, http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top).

[20] Senator Amy Klobucher, Hearing, U.S. Senate Committee on Commerce, Science & Transportation, February 5, 2015; 1:23:38- 1:24:30.