

GEORGE JEPSEN
ATTORNEY GENERAL



55 Elm Street
P.O. Box 120
Hartford, CT 06141-0120

Office of the Attorney General
State of Connecticut

November 16, 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. You have exercised your discretion in collectively moving to chip and signature, and we now call on you as the key decision-makers to move to the full chip and PIN technology as soon as possible. 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. We urge you to act more quickly to implement an 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 breaches² 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.

A report issued by the New York Attorney General’s office last year revealed that more than 900 data security breaches exposed the personal records of 7.3 million New Yorkers in 2013. These breaches cost entities conducting business in New York upward of \$1.37 billion. Although the report found that hacking intrusions were the leading cause of data security breaches, lost or stolen equipment or documentation (including credit or debit cards) accounted for nearly 24% of the data breaches in New York in 2013.

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, 2015).

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.*

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

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.

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).

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.”)

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. 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 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

Although adopting a PIN-based system would not have prevented all of the recent data breaches, experts and advocates agree that chip-and-PIN cards will best protect consumer information during point-of-sale transactions. According to Consumers Union, total fraud losses dropped by 50 percent and card counterfeiting fell by 78 percent in the first year after EMV smart cards were introduced in France in 1992.¹⁹

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.²⁰ In the wake of recent wide-scale data breaches, information came to light indicating that credit

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>).

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.”). Alarming, 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 See http://consumersunion.org/wp-content/uploads/2014/02/Privacy_Digital_Age_Testimony_020414.pdf

²⁰ 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>).

and debit cards issued in this country were more valuable on the black market because these cards lacked chip technology.²¹ Of course, all stakeholders – businesses, individuals and your institutions – can and should do much more to better protect against data security breaches. 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.

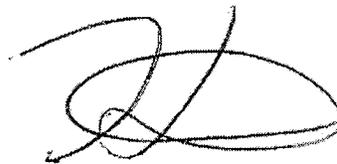
The purpose of this letter is not to suggest that Chip and Pin or any other particular technology should be enshrined in federal or state law as a legal mandate on card issuers. Rather, this letter calls upon you as good corporate citizens to voluntarily expedite the implementation of existing technology that offers the most substantial security benefits, and to continue to adapt and improve security as quickly as possible as technology advances. Indeed, we are sensitive to the concern that locking into the law any particular card security technology may pose risks to future innovation and/or give rise to incompatible technical requirements in different jurisdictions. Those concerns should be evaluated if and when they arise in the context of particular legislative proposals, and this letter should play no role in evaluating them. Nor do we seek to identify or impose a date certain by which Chip and Pin should be implemented. We recognize that you must and should consider disruptions to consumers and retailers and take steps to minimize them. That said, we believe you can move more quickly to implement Chip and Pin as an important security improvement, and we urge you to act with all deliberate speed to do so.

Again, we urge you to 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.

Sincerely,



GEORGE JEPSEN
Connecticut Attorney General



KARL A. RACINE
District of Columbia Attorney General

²¹ Senator Amy Klobuchar, Hearing, U.S. Senate Committee on Commerce, Science & Transportation, February 5, 2015; 1:23:38- 1:24:30.



LISA MADIGAN
Illinois Attorney General



JANET T. MILLS
Maine Attorney General



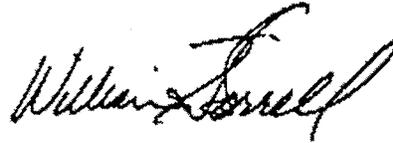
MAURA HEALEY
Massachusetts Attorney General



ERIC T. SCHNEIDERMAN
New York Attorney General



PETER F. KILMARTIN
Rhode Island Attorney General



WILLIAM H. SORRELL
Vermont Attorney General



BOB FERGUSON
Washington Attorney General