



Timothy J. Heine
Managing Counsel
General Counsel's Office

American Express
World Financial Center
200 Vesey Street
New York, NY 10285-4908
Tel: 212.640.5745
Fax: 212.640.0364
Internet: tim.heine@aexp.com

February 5, 2014

The Honorable Al Franken
United States Senate
Washington, DC 20510

Dear Senator Franken:

Thank you for your letter dated January 15, 2014, which presented your concerns regarding the security of American consumers' payment cards and a number of related questions on payments systems and EMV adoption in the U.S. We appreciate the time you have taken to raise your concerns with us and the opportunity to respond to your questions.

As you know, fully implementing EMV in the U.S. requires a number of interdependent parties working together, including card issuers, merchant acquirers, processors, merchants and ATM and debit networks. Critically, each stakeholder group along the U.S. payments chain is working together to ensure the new EMV eco-system will operate in a secure and effective manner. For example, card issuers are issuing EMV-enabled products, merchants are making hardware and software upgrades, and processors and networks are providing end-to-end certification at merchant locations to ensure these transactions can be processed. The U.S. is the largest and one of the most complex markets undergoing an EMV migration, and American Express is committed to working alongside other industry stakeholders to establish a secure and fully interoperable environment for EMV payments.

American Express has a unique position in the payments industry as we operate as a card issuer, a merchant acquirer and a payments network, in addition to partnering with other financial institutions that issue cards and acquire merchants on our network. This is in contrast to others in the industry that may act, for example, solely as a card issuer or as a network. Since



February 5, 2014

Page 2

announcing our EMV roadmap in 2012, American Express has been working across multiple fronts with all of our key stakeholder groups to help advance the migration of EMV payments in the U.S.

First, as a global payments network, recognizing the complexity involved in migrating to EMV chip-based technology, we aligned the dates of our U.S. EMV roadmap and policy fulfillment to those of other payments networks. In doing so, we are able to facilitate the migration process so that, for example, American Express' EMV specifications may be certified alongside those of other industry participants to optimize migration efficiencies. In addition, we have been working closely with our U.S. card-issuing partners to certify them for EMV-enabled transactions on our network.

Second, on the merchant acquiring side of our business, we have been working actively with both our processing partners and our merchants to certify them for EMV transactions on our network. To date, the vast majority of our partners' processing platforms now support EMV, and we continue to work closely with our merchants to certify them for EMV transactions.

Third, as a card issuer, beginning in mid-2013, American Express' consumer, small business and corporate card-issuing divisions began issuing EMV-enabled chip and signature cards on a select basis. Later this year, all of American Express' consumer and small business credit and charge products will become available with EMV chip and signature for Card Members who request them. American Express' Gold, Platinum and Centurion Corporate Card products are now available with EMV chip and signature; Green Corporate Cards with EMV chip and signature will continue to be offered on a select basis. Ultimately, as the full EMV infrastructure becomes established in the U.S., American Express' EMV-enabled products will be provided to our Card Members through our ongoing card renewal processes, and our prepaid products also will be available with EMV chip technology.

In addition to our more recent efforts to migrate to EMV in the U.S., American Express continually has been at the forefront of deploying best-in-class fraud management capabilities that detect or prevent fraudulent activity on our network. For example, many large retail chains have deployed our Card Member verification tools at the point of sale, which has resulted in a decrease in fraud losses at those chains by more than 70 percent. Our fraud management efforts also focus on online transactions for which EMV does not provide the same benefits vs. transactions at physical merchant locations. In addition, we also have made it easier for our Card Members to monitor their accounts for fraudulent activity through notifications that are delivered in real-



February 5, 2014

Page 3

time via email, SMS message and smart phone app push notification. We are continually enhancing our fraud monitoring systems and controls to adapt to the constantly changing and increasingly complex activities of fraudsters. These efforts, coupled with our policy to not hold our Card Members liable for any fraudulent charges, give our customers confidence that their accounts are protected.

Across the e-commerce arena, American Express also is continually providing new ways to combat fraud and provide a secure environment for American Express Card Members shopping online. For example, as an equity owner of EMVCo, a global technical organization, American Express is working closely with the broader payments community to develop a new global tokenization standard that would provide enhanced security for consumers making payments online through a personal computer, mobile phone or other smart device.

At American Express, we view EMV technology as an important tool, among many, that we use to deliver a multi-layered detection and prevention strategy for fraudulent transactions at the point of sale. Combating fraud is a constant and ever-changing battle, which is why it is more important than ever that card issuers, processors, payment networks and merchants continue to work together to address these ongoing fraud threats.

We thank you again for reaching out to American Express for our views on this important issue. Should you need any further information, please contact Chris Merida in our federal government affairs office in Washington, D.C. at 202-434-0157.

Sincerely,

A handwritten signature in black ink, appearing to read "Timothy J. Heine", with a stylized flourish extending to the right.

Timothy J. Heine, Esq.
Acting General Counsel

John Collingwood
Senior Vice President
Federal Government Relations

February 5, 2014

Honorable Al Franken, Chairman
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Franken:

Thank you for the opportunity to respond to your inquiry concerning the security of American consumer payment card data. Bank of America is committed to protecting all consumer data and to providing consumers with a secure experience when using their bank payment cards. As a reflection of our commitment, we have been honored to be ranked #1 in overall fraud prevention for the seventh consecutive year by Javelin Strategy and Research in their [Credit Card Issuers' Identity Safety Scorecard](#), which analyzes the customer-facing security features of 24 of the nation's top credit card issuers.

We have achieved these rankings by intensely focusing on the larger issue of customer data security. We make significant investments every year in fraud monitoring, detection and prevention systems and constantly develop and improve technology, processes and procedures to protect our customers. In the event of consumer data breaches like the one that occurred recently at Target, as a matter of routine, we identify which customers may have been affected, monitor their account activity and, if appropriate, reissue their cards. We offer all customers our Zero Liability Guarantee and provide customers with a variety of fraud alerts through several channels—all at our expense. More broadly, we work closely with government and industry peers to ensure that we are adhering to Gramm–Leach–Bliley Act (GLBA) requirements and Payment Card Industry Data Security Standards (PCI-DSS), both of which are integral parts of enhancing the security of customer and payment data. Further, we have a long history of working closely with law enforcement and, of course, we continue rolling out cards with EMV-chip technology.

We believe data security is a much broader issue that goes well beyond the processing of payments. In regard to the payments systems, there are a number of steps that can and should be taken to strengthen security. However, no single solution by itself (PCI-DSS, encryption, EMV-Chip, etc.) will provide absolute protection. For example, EMV-chip technology does not solve the growing threat of card-not-present fraud, which is experiencing significantly elevated fraud losses as point-of-sale transactions become more secure and online transaction volume increases. To succeed in

Tel: 202.661.7130 • Fax: 202.661.7110
john.collingwood@bankofamerica.com

Bank of America, DC8-455-09-01
1455 Pennsylvania Avenue, NW, 9th Floor, Suite 950, Washington, DC 20004-1043

combating these threats, security measures must continually evolve. There must be a coordinated and sustained effort among the key stakeholders — card networks, payment processors, retailers as well as banks — to provide reliable and secure data collection and payment systems that consumers can trust as well as find convenient to use.

Status of Bank of America's Transition to EMV-Chip Cards

Bank of America is committed to and is deploying EMV-chip technology across our consumer and small business card portfolios. EMV-chip cards will help bring enhanced security to cardholder data and will provide greater flexibility for international travelers. In order for EMV-chip technology to have maximum effectiveness, though, there needs to be end-to-end adoption of the technology by banks, networks and equally as important, by the acquirers and retailers, both here and in many other countries around the world.

Bank of America began deploying EMV-chip cards to consumer and commercial credit card customers in 2012. For select products, EMV-chip is a standard feature on newly opened credit card accounts and is available at customer request on many of our existing credit card accounts. We continue to migrate more of our customers to EMV-chip enabled cards as well as provide a number of other security enhancements to help protect customers' information and enhance their payment experience.

The deployment of EMV-chip cards within the U.S. debit card market remains a priority for Bank of America as well. Prior to a recent decision in the ongoing litigation over debit interchange and network routing requirements, Bank of America was evaluating an EMV-chip conversion ahead of the October 2015 liability shift dates put in place by the payment networks. The uncertainty of current litigation and the complexities in working toward a common industry solution to allow EMV-chip technology to have more than one unaffiliated debit network on which transactions can be routed has resulted in industry-wide delays. Bank of America is working diligently with payment networks and industry stakeholders to help establish an industry standard for this new requirement so that EMV-chip debit cards can be delivered to our customers in an efficient and measured manner, but, as mentioned, uncertainties do remain.

Main Impediments to Adoption of EMV-Chip cards and Other Security Improvements

The timing of EMV-chip deployment is directly influenced by the rate of adoption of EMV-chip technology across the entire payment system (by retailers, processors, etc.), the ability to add EMV-chips to existing payment cards without major customer inconvenience or confusion, and finalization of industry standards that may be affected by additional regulatory requirements and/or legal settlements.

Broad adoption and use of EMV-chip cards is dependent on all stakeholders in the payment system (retailers, acquirers, networks and banks) investing in, implementing and using the technology together. When fully deployed, the EMV-chip technology will enhance the "checkout and pay" experience by consistently enabling safe, reliable and efficient point-of-sale transactions. However, until there is universal end-to-end adoption by all of the stakeholders, the value and impact of EMV-chip technology will not be maximized. To ensure that consumers can continue to use payment cards at all physical retailer locations—even those that have not converted to EMV-chip readers—EMV-chip enabled cards will still need to include a magnetic stripe. In addition, EMV-chip technology does not solve the growing issue of card-not-present fraud, which is experiencing significantly elevated fraud losses as point-of-sale transactions become more secure and a larger portion of consumer commerce is conducted online.

Costs and Benefits of Expediting the Transition to EMV

There exists presently a tight timeline laying out the payment card industry's EMV-chip adoption roadmap, especially in light of several industry uncertainties. Expediting the transition further is only meaningful if every component of the entire system is also expedited. The benefits of end-to-end EMV-chip technology clearly will provide greater security, especially for point-of-sale transactions, and we are committed to that outcome. Other stakeholders can better address the cost or other concerns for the transition of components beyond our control.

Broader Improvements to Protect Customer Data and Prevent Fraud

Every year we make significant investments that are focused on allowing customers ease of access to their funds while preventing and detecting potential fraud. If customers have their card information stolen or become victims of fraud, we will assist them to resolve it effectively and offer information and tips to help protect themselves against these and other types of fraud threats. We invest hundreds of millions of dollars every year to enhance our fraud prevention and detection capabilities to avoid unauthorized access to customers' funds. Further, we recognize that our customers not only expect to be protected from fraud, but also want payment systems that are efficient and convenient and we design our systems accordingly.

For example, our customers are in the best position to know when and where they have made transactions. Thus we continue to invest in text, email and call center tools to improve the reach and speed at which we contact customers when fraud is suspected while offering them a highly efficient process to confirm legitimate activity and continue using their cards. These investments expand our ability to reach customers quickly wherever they may be, and allow them a discreet and efficient way to resolve situations where fraud may have occurred.

Bank of America is committed to providing American consumers with a secured experience when using their bank payment cards. Continuing the transition to EMV-chip enabled technology across issuers, networks, payment processors and retailers is an important part of this commitment. We also believe customer data security is the broader issue and that it goes well beyond the processing of payments, touching retailers and financial institutions alike. In regard to the payments system, there are a number of steps that can and should be taken to strengthen security. However, no single solution by itself will provide full protection. To succeed in eliminating data breaches, technology and security measures must continue to evolve. There must be a coordinated and sustained effort among all the key stakeholders—card networks, payment processors, retailers as well as banks—to continue to provide a reliable and secure payment system that consumers can trust.

Sincerely,



John Collingwood
Federal Government Relations Executive



Capital One Financial Corporation
1680 Capital One Drive
McLean, VA 22102

February 4, 2014

The Honorable Al Franken
Chairman, Subcommittee on Privacy, Technology, and the Law
309 Hart Senate Office Building
Washington, DC 20510-2309

Dear Senator Franken:

Thank you for your letter and your leadership in pursuing ways to create a more secure payment system in the U.S. In particular, Capital One agrees with your observation that the evolving threats to our payment systems support adoption of more secure card technology in the U.S. – including EMV cards that are already widely used in Europe and other regions today.

It is important to note that, even with the widespread use of magnetic swipe technology in the U.S., Capital One has numerous processes in place to minimize payment card fraud. For example, our systems are programmed with literally hundreds of fraud algorithms designed to detect and prevent unusual transaction activity, which trigger wide range of fraud mitigation steps – such as confirmation calls to our customers, temporary usage blocks, permanent usage blocks, and other responses. Also, as you know, our customers face zero liability for fraudulent charges to their accounts.

Nonetheless, we believe that it is important to constantly improve our processes to reduce payment card fraud and the development of EMV technology is an important security enhancement. In a world in which a significant number of merchants still use magnetic swipe technology, the demand within the criminal marketplace for stolen payment card data will still thrive. Card data stored on EMV chips is more secure because the information, even if stolen, cannot be used to initiate fraudulent transactions on EMV-capable terminals. In the past, EMV technology has been plagued by a “chicken-and-egg” dilemma because EMV technology only reduces fraud if the overwhelming majority of retailers adopt point of sale technology that accepts EMV payment cards. Simply put, banks have been historically reluctant to invest in payment card EMV technology without retailer adoption and retailers have been historically reluctant to invest in point of sale technology without bank adoption of EMV cards. This is why the development of EMV technology is a shared responsibility between the banks and the retailers.

Fortunately, the two largest payment networks (Visa and MasterCard) have now created a framework of market-driven incentives to address this challenge. The new payment rules require payment card issuers and merchants to adopt EMV technology by October, 2015, in order to minimize their own liability for payment card-related fraud losses. As outlined below, Capital One is both committed to EMV issuance and fully supportive of this timeframe.

In response to your specific questions:

1. What is the status of your institution's transition to EMV cards?

Capital One is currently building the technological infrastructure necessary to roll out EMV cards. Of course, rolling out a new technology to more than 40 million card holders is a significant undertaking and it must be executed to precise standards. Our customers rely on their payment cards to make important payments every day (including paying for groceries, gas, and health care products) and whether they're at home, in their local community, or traveling, we want to make sure those payments are made without disruption.

To that end, we will first roll out EMV credit cards in the U.S. to a pilot group of customers to ensure that our operational systems work as planned before rolling out EMV cards to all of our customers. Our current plan is to begin this pilot in mid-2014.

Although Capital One is a relatively small player in the debit card space, it is important to note that EMV adoption for debit cards is on a slower trajectory because of pending litigation over the Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. Specifically, the U.S. Court of Appeals for the D.C. Circuit is currently considering, among other things, the appropriate interpretation of the Durbin Amendment's requirement that debit cards be processed on more than one network. The outcome of that ruling will impact requirements for routing debit transactions and therefore how we implement debit EMV. We currently intend to conduct a pilot of EMV technology for our debit card program in late 2014.

2. When will all cards issued by your institution be EMV card or include similar security features?

We anticipate that newly issued credit and debit cards will contain EMV technology during 2015. However, it will take longer to convert all existing cards because of the rolling nature of card reissuances.

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?

The MasterCard and Visa rules provide incentives for issuers and merchants to adopt secure payment methods. For example, retailers are being incentivized to adopt EMV technology by October, 2015 in order to minimize liability for fraud losses. Given the recent challenges faced by some large retailers, we believe these incentives will be effective in encouraging the adoption of point-of-sale EMV technology by retailers. With respect to consumer adoption, we intend to educate our customers about the benefits of EMV technology as part of our rollout of EMV payment cards. We will explain to our customers that, while they are already protected from payments on fraudulent charges, the new cards will afford additional protections against fraud. Our 2014 customer pilot will help us fine tune this education campaign.

4. Could you expedite your transition to EMV cards? What would the costs and benefits be doing so?

We could expedite our transition to EMV cards if we launched a full roll out without first piloting the technology to ensure reliable operational execution and a favorable customer experience. We do not intend to take this course. Pilot testing new technology is essential to help identify any unintended operational challenges and rolling out EMV technology before we know definitively that it will work exactly as expected could be very disruptive to our customers – perhaps even souring our customers on the benefits of EMV technology. Moreover, because retailers have not yet adopted point-of-sale EMV technology in a significant way, there would be limited meaningful benefit to customers.

5. What other improvements are you pursuing to protect consumer data and prevent fraud?

Capital One has a robust Information Security Program that includes, among other features: hundreds of system algorithms designed to identify suspicious transactions; multifactor online authentication; secondary authentication for high-risk transactions; multi-factor mobile authentications; 24/7 post-fraud account suspension; and various types of activity alerts. We make continuous investments and improvements to our program and we also collaborate with payment networks and other banks to help identify and prevent fraud. Although it is impossible to list here all the existing and evolving algorithms we use to identify and mitigate fraudulent transactions (and it is of course important that we keep our fraud algorithms confidential to avoid criminal detection), we would be pleased to meet with you or your staff to explain some of our processes in person.

It is also important to note that we take numerous steps to educate our customers about things they can do to help protect themselves and reduce the risks of falling victim of fraud. For example, our website includes the following Tips to Prevent Fraud on Your Credit Card or Debit Card:

- Never leave receipts behind where someone could pick them up – especially ATM, supermarket, and self-service gasoline pump receipts. Also, never let anyone put your account number on a check or any other document not associated with a purchase on your account. (In some states, this is against the law.)
- Never give your account number to someone calling you on the phone, even if the caller says it will be used to claim a prize or award.
- Store your credit card and/or debit card in a secure place where you will immediately know if it is missing.
- Sign the back of your credit card and/or debit card as soon as you receive it.
- Never leave your credit card and/or debit card as a "security deposit" or as identification. Instead, use your driver's license.
- Never lend your credit card and/or debit card to anyone.
- When you are expecting a new or replacement credit card or debit card, look for it in the mail.
- Report a lost or stolen credit card or debit card immediately.

The Honorable Al Franken
February 4, 2014
Page 4

- Never carry your PIN in your wallet or write it on the back of your credit card or debit card, and don't choose an obvious number (such as your birth date or telephone number) for your PIN.
- Review your credit bureau reports regularly. This may be the only way to identify if you are a victim of identity theft.

More information is available by searching "Fraud and Identity Theft" at www.capitalone.com

6. What are the main impediments to the adoption of EMV cards and other security improvements?

As discussed above, significant work is still required by both banks and merchants in order to achieve widespread adoption of EMV technology. However, the recent retailer data breaches have fueled the momentum towards EMV adoption and we are optimistic that both partners are highly motivated to make the transition and make it work.

Finally, we believe that consumer education will be essential for the successful transition to EMV technology. Capital One plans an extensive effort to ensure a positive customer experience with the new technology, but we will all have to work with consumers to explain the shift to EMV cards and how they work. Indeed, as retailers and banks consider future options for the evolution of payment security, customer experience will be a major factor in the ultimate success of any new technology.

On behalf of Capital One, I want to thank you for the opportunity to provide this information. This issue is of great importance to Capital One, the entire payment card industry and its customers and we appreciate your concern for, and efforts to better understand our plans to employ the technology. We would be happy to discuss these issues in greater detail with you, or your staff, at your convenience.

Sincerely,



Ryan Schneider
President, Card

CC: Senator Jeff Flake, Ranking Member
Senate Subcommittee on Privacy, Technology, and the Law



February 4, 2014

The Honorable Al Franken
309 Hart Senate Office Building
Washington, DC 20510

Dear Senator Franken,

Thank you for your letter of January 15, 2014 regarding data breaches and card security. I want to assure you that Citi takes the security of our customers' information and our nation's payment infrastructure most seriously. The firm as a whole invests a significant amount of time, energy, and resources to put high standards and safeguards into place.

Multiple parties are involved in making the payments system work for American consumers, including card issuing banks, payments networks, merchant acquiring banks, payment processors, and merchants/retailers. As a financial institution, we recognize our important role in the security of the payments system and Citi, along with others in our industry, dedicates millions of dollars and significant human capital and technological resources towards data security, fraud prevention and – most importantly – the protection of our customers. Moreover, we shield customers who use our credit and debit products from liability for fraud that is perpetrated on their accounts, providing them with further peace of mind when using their card.

Financial institutions are subject to comprehensive oversight and examination from a variety of regulators, which we believe only further helps to strengthen our processes. In the current environment, banks are the only payments system participants subject to this level of rigorous oversight.

On a daily basis, Citi protects our customers in many ways from fraud and data breaches, which vary in criminal technique and scale of impact. Customer protections include, but are not limited to:

- Continuous transaction and account activity monitoring
- Fraud alerts
- Zero customer liability for fraud
- Free Identity Theft and Victims Assistance Programs to help customers reclaim their identity and re-establish credit

When a data breach is identified, we work quickly to minimize disruptions to our customers. This starts by identifying accounts that may be at risk and then increasing the sensitivity of our transaction monitoring on those accounts. Further, we communicate with our customers, encouraging them to immediately contact us if they believe there could be fraudulent activity on their account and notifying them how to protect their information.

Reissuing a card is a complex decision and can cause inconvenience to customers. We take these decisions very seriously and use a balanced approach in our evaluation of the risk involved and potential customer impacts. We want to avoid adverse customer impacts such as service interruptions or limited access to their accounts. For example, where customers have automated recurring transactions, we do not want them to be required to change billing information unless absolutely necessary.

One of many tools to combat fraud is EMV or chip cards. This card authentication tool helps reduce counterfeiting of cards; however, that is not the only threat to consumers and our payment infrastructure. The EMV transition is underway, yet requires shared responsibility, standards, and investment by all parties.

QUESTIONS

1) What is the status of your institution's transition to EMV cards?

Citi began the transition to EMV cards in North America with a pilot in 2011 and the production rollout began in late 2012. We are making significant progress: 7 million of our MasterCard and Visa cards have been reissued as EMV products to date. We are committed, and have urged the rest of the industry, to maintain the timelines established by the payment networks. We completed the upgrade of all of our North American ATM terminals with EMV technology in April 2013.

2) When will all cards issued by your institution be EMV cards or include similar security features?

Citi is planning to have the vast majority of our MasterCard, Visa, and American Express products reissued with EMV cards by the end of 2015. We are actively issuing EMV cards for new accounts and normal reissues for a number of our products, with additional segments to follow throughout 2014 and 2015. The true protection of these cards will only come into play when all partners in the payments system adopt the technology and make it usable for customers.

3) What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?

Citi has many retail partners and we work closely with them on many issues including the customer experience and security. For example, we have partnered with one large retailer to require CVV2 (an additional numeric authentication code on the signature strip) on Card Present transactions to improve the security of that transaction.

We also have made significant investments in hardware, software, and customer communications. Citi provides ongoing security information for customers at:

<https://online.citibank.com/US/JRS/pands/detail.do?ID=SecurityCenter>.

We are also actively engaged in industry forums that advocate EMV chip card adoption across the payment system.

The payment networks (MasterCard, Visa, and American Express) may have more information than we do (as an issuing bank) regarding incentives for merchant adoption and liability changes associated with their timeline.

4) Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?

Successful migration to EMV cards is dependent upon merchant acceptance of these products. Since acceptance of EMV cards at the merchant point of sale is still very low in the United States (less than 1%) there is minimal value in accelerated reissue at this point, as consumers would not have the protections associated with this technology until merchants adopt the terminals. Costs associated with implementing EMV cards have been built into our business plans.

5) What other improvements are you pursuing to protect customer data and prevent fraud?

Citi is constantly evaluating and investing in tools to improve fraud detection and protect our customers' information. As an example, in 2014, we are upgrading our North America fraud detection platform capabilities across all of our consumer card products.

6) What are the main impediments to the adoption of EMV cards and other security improvements?

The current industry migration timelines guide both issuing banks and merchants to migrate by late 2015.

As mentioned, the largest initial impediment to adoption of EMV cards is ensuring that all members of each group adopt the technology. If any issuer or members of the merchant community do not adopt the technology, vulnerability for criminals to exploit will remain in the payments system.

The debit market is in flux given significant pending regulatory and judicial rulings. These uncertainties make it challenging to plan for EMV reissue and timelines of debit cards, especially while considering the impact to the customer experience.

There is a large consumer education effort that will go along with a transition to EMV payment cards. Communications with consumers will focus on increasing awareness of the product and its associated benefits, as well as providing information on where and how to use the product. Training and understanding are also required of in-store associates and customer service agents to ensure they can effectively explain the technology to consumers and help to address any concerns.

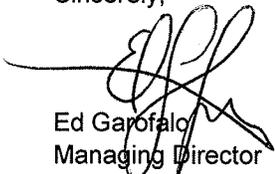
Finally, EMV is not a solution for all fraud – it only reduces counterfeiting. Many transactions are processed either when the card is not present or online, which will not be addressed by EMV chip card. Criminal threats continue to evolve and grow in sophistication and all parties in the electronic payments system need to constantly keep pace with the changing threats. EMV chip cards are an excellent tool in the fight against counterfeiting, especially once all those in the payment ecosystem have adopted the technology. It will provide additional cardholder verification, devalue the account number by providing unique transaction information, and lay the groundwork for future innovation.

Citi continues to invest in strong data security. We are an advocate for better safeguards across the industry and are dedicated to protection of information within our control. We know that criminals will continue to look for vulnerable aspects of the payments system, whether this is merchants who do not implement EMV terminals, Online, Card Not Present transactions, stored personal data, or other threats. All participants in the payment industry must continue to evolve their security efforts and not rely on one solution to protect the system and consumers. Consumer confidence in our payments system is crucial – not only do their transactions need to be secure, but they need to be aware of and understand the protections provided on their behalf – by all participants in the system.

Everyone in the payment infrastructure has a responsibility to protect the system and consumers. We all rely on the other partners in the payments system to take their responsibility seriously. Citi is committed to continuing to work with the networks, law enforcement, and merchants to better understand the impact of breaches and determine the best strategies to protect customers.

Thank you for your letter and continued interest in our secure payments environment.

Sincerely,



Ed Garofalo
Managing Director
North America Risk Operations

Citi, the leading global bank, has approximately 200 million customer accounts and does business in more than 160 countries and jurisdictions. Citi provides consumers, corporations, governments and institutions with a broad range of financial products and services, including consumer banking and credit, corporate and investment banking, securities brokerage, transaction services, and wealth management. Additional information may be found at www.citigroup.com | Twitter: @Citi | YouTube: www.youtube.com/citi | Blog: <http://blog.citigroup.com> | Facebook: www.facebook.com/citi | LinkedIn: www.linkedin.com/company/citi



February 5, 2014

Senator Al Franken
United States Senate
Senate Hart Office Building
Room 309
Washington, D.C. 20510-2309

Re: Payment Card Security

Dear Senator Franken:

I am writing in response to your January 15, 2014 letter regarding the security of payment card data.

This is a topic that is extremely important to us as it relates to our core businesses. Discover is unique in that we are not only a major issuer of credit cards, but also operate both a credit card network (Discover Network) and a debit card network (PULSE) that process debit transactions for thousands of banks and credit unions. For all of these businesses, it is critical that there be a high level of security both for payment cards themselves and for the information that flows from consumers to merchants and their banks, to card issuers and to third parties that facilitate the transmission of data through the payments infrastructure.

Your letter focuses on one element of payment data security - the security of payment cards themselves - but it also refers to other strategies for safeguarding consumer data. We agree that a multi-faceted approach is critical: criminals who seek access to consumer financial information exploit vulnerabilities wherever they exist and adjust their tactics to find new points of entry into the system as older ones are closed off. No single security measure can address all threats or even permanently address the known vulnerabilities they are designed to combat.

An important tool in the battle against data breaches addresses the security of payment card information when it is in the hands of merchants, processors and others. The Payment Card Industry Security Standards Council ("PCI"), launched in 2006, works with all participants in the payments infrastructure to devise standards for the use, storage and transmission of payment data. Discover and the other card networks have collaborated in the development and evolution of the PCI standards, share in PCI's governance, and have adopted the PCI standards as the foundation for the security requirements they expect merchants who accept their cards to adopt. Merchants, depending on their size and other attributes, certify their PCI compliance, including through PCI compliance evaluations conducted by independent assessors. The security of the payments ecosystem has improved since the

introduction of the PCI standards. In particular, most merchants are no longer storing card numbers, a practice that had been the source of earlier large data security breaches.

Contributing to the strength and effectiveness of PCI is its operation as an open, collaborative forum involving both the networks and hundreds of industry participants. Payment networks have worked together, devoting considerable resources to the development of state of the art defenses against criminal access to payment card information. PCI participants license technology they develop without fees or limitations on usage. Shared ownership and collaborative development have encouraged innovation and strengthened the ability of all participants to combat data breaches.

It is our hope that EMV migration and evolution will take place in a similar environment, despite signs that this is not occurring. In contrast to past security enhancement efforts, key decisions relative to the EMV rollout are not being managed by an independent body, like PCI, with participation of all affected entities, including, of course, the merchants who will bear new liability for fraud under EMV. Instead, they have largely been in the hands of the dominant payment networks which are dictating standards and applications. While Discover's application has been made available under open terms, other networks' EMV applications are being offered through time-limited licenses with restrictive terms. As a practical matter, a common application must be adopted to avoid incompatibility issues. It is essential that it be truly open and free of restrictions that favor a single entity.

The EMV "chip" card is an effective tool to combat the manufacture and use of counterfeit cards. Counterfeiting such cards is currently far more difficult than producing cards with data that is "skimmed" from the magnetic stripes of genuine cards or stolen from merchants, card issuers, processors or others. But it does not address all vulnerabilities. Unless a chip-enabled card also requires the entry of a PIN to validate that the person presenting the card is an authorized cardholder - a requirement outside the United States - it has limited ability to thwart fraud by criminals and others who use genuine cards that have been lost, stolen or "borrowed" - still a very significant source of fraud. Signature authentication does not accomplish this: a thief can fake a signature, but not a PIN, whether the card is validated offline or directly with the issuer at the time of the transaction. The introduction of chip plus PIN cards in the U.K. resulted in a very significant reduction in card-present fraud.

A chip-enabled card has limited utility as a fraud protection measure in "card not present" transactions, such as the growing number that take place over the Internet or via mobile phones. Other technologies that perform the PIN function are needed to authenticate that the online/mobile cardholder is in fact an authorized user. Some of these are still in development (e.g. data-generating "tokens," biometric identifiers) and represent the next generation of security.

With respect to Discover's implementation of EMV, we expect that by October 2015, a significant portion of our active Discover Cardmembers will be converted to EMV chip-enabled cards, at a considerable cost. Later this year, we plan to issue EMV cards to our internationally-traveling customers for use in countries where EMV terminals have been widely deployed. Our payments networks notified

merchant acquirers in 2013 that point-of-sale terminals must have the ability to transmit EMV-formatted transaction information effective October, 2015 (October, 2017 for petroleum merchants).

In the U.S., less than 1% of merchants currently have EMV capability. Accelerating the issuance of EMV cards will not benefit consumers unless merchant acceptance of those cards is in place. To incentivize merchants to deploy it, Discover, like the other networks, has announced a fraud liability shift under which merchants and acquirers that do not deploy EMV terminals will be liable in the event of "card present" losses. This strategy has been successful outside the U.S. Discover has also offered incentives to issuers and merchants who adopt the additional security requirement of PIN authentication.

Finally, large debit card issuers have indicated that an impediment to an earlier EMV conversion date is uncertainty about the outcome of the legal challenge to the Federal Reserve's Regulation II (implementing the Dodd-Frank requirement that debit card transactions be routed over multiple payment networks). Their views should be taken into account in evaluating the impact of accelerating the EMV timeline.

I appreciate your interest in these issues and would be pleased to provide further information.

Very truly yours,

A handwritten signature in black ink, appearing to read "David W. Nelms". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

David W. Nelms
Chairman and Chief Executive Officer

JPMORGAN CHASE & CO.

February 5, 2014

Honorable Senator Al Franken
United States Senate
309 Hart Senate Office Building
Washington, DC 20510

Dear Senator Franken:

Thank you for your January 15, 2014 letter to James Dimon, Chairman and CEO of JPMorgan Chase & Co. ("Chase"). Chase welcomes the opportunity to respond to your inquiries, and to share with you additional information regarding payment network data security and our current and contemplated practices, including with respect to Europay MasterCard Visa ("EMV") technology.

Chase shares your concerns about evolving security threats to U.S. payment systems. As you note in your letter, we, and others in the financial services industry are working to improve card payment security and, as discussed in more detail below, have made notable progress on a number of fronts, including EMV and other technologies. However, as recent events demonstrate, there is more to be done across the marketplace, including completing the transition to EMV technology as soon as practicable, which Chase fully supports.

It is in everyone's best interest, including Chase's, to fully implement EMV technology throughout the U.S. card-based payment system in an expedited fashion. However, as you note, the transition to EMV technology must be handled in a way that ensures the advantages it offers are as effective as possible. As discussed in more detail below, there are several significant challenges to overcome in order to fully and effectively transition to EMV technology. Proceeding before these challenges have been resolved will result not only in a less effective implementation, but likely also will cause significant extra expense for card issuers and merchants in the form of multiple card re-issuances, repeated equipment replacements and/or re-programming, as well as significant inconvenience to cardholders.

Chase will do all it reasonably can to help all stakeholders overcome these challenges and to identify, develop and implement additional solutions designed to make the U.S. payment systems more secure, convenient and reliable for consumers, merchants and financial services providers.

You understandably have asked several questions about EMV technology. To help put our responses to your questions in the broader context we want to provide a high level overview of EMV technology and certain aspects of the U.S. payment card system.

What Is EMV Technology

Each EMV-enabled debit and credit card contains a built-in security chip that utilizes a form of cryptography to authenticate the card, card issuer and the data stored on the card. The chip itself performs three key functions: (i) stores information, (ii) performs transaction – related processing, and (iii) provides cryptographic authentication that helps protect sensitive data. EMV technology allows card issuers and merchants to verify the card’s authenticity during each transaction, and when combined with a PIN or signature to verify the cardholder’s identity, results in a higher degree of certainty that the transaction is not fraudulent.

To implement EMV technology, credit and debit cards must carry the security chip, and point-of-sale terminals where the cards are presented must be able to read the chip. Historically, card issuers have borne the cost of issuing and replacing cards, and merchants have borne the cost of purchasing and maintaining the point-of-sale terminals.

Other Considerations

As noted above, EMV is the latest technology for point-of-sale terminals, offering more security to help prevent card skimming, counterfeit replication and other types of “card-present” fraudulent attacks and indeed, has proven to be a significant tool in the effort to reduce marketplace fraud for card-present transactions. However, EMV technology is only part of the solution and will not preclude all fraudulent credit and debit card transactions. In particular, EMV will not reduce fraud in connection with “card-not-present” transactions. In fact, the migration to EMV technology likely will result in increased card-not-present fraud. In Europe where EMV is more widely utilized, fraud has shifted from card-present transactions to online, card-not-present transactions. Given the ongoing expansion of online shopping the marketplace must develop one or more separate solutions to protect against fraud aimed at these transactions. To this end, Chase is investing in “tokenization” solutions that will enhance the effectiveness of our anti-fraud efforts for both card-not-present and traditional card-present retail transactions. With tokenization, when a consumer enters their card number into a web or mobile site for payment, instead of being used directly, the card number is transformed into a cryptographic “token” that cannot be used for any purpose other than that single transaction. The token, therefore, is useless to criminals who may steal the token in transit, or through a data breach.

Furthermore, U.S. payment systems comprise a wide variety of participants. In addition to the traditional parties (issuing banks, card networks, merchants/retailers, merchant acquirers, processors) there are a number of newer non-bank entrants providing mobile payment solutions, electronic wallets, online payment tools and related services. Banks are subject to robust regulatory examination and oversight to safeguard consumers, as well as meaningful capital requirements; the same is not true for many of the newer, non-bank entrants. It is imperative that any solution addressing payment network security include a clear set of rules, and consistent regulatory standards for all payment system and market participants.

Moreover, security protocols and transaction processing requirements impact all of these participants and each must be involved in developing solutions and uniform standards. If not, transaction processing security, efficiency and cost will be adversely affected.

Responses to Your Inquiries

1. What is the status of your institution's transition to EMV cards?

Credit Cards

Chase currently has more than 1.7 million EMV-enabled credit cards issued out of approximately 75 million cards in circulation. Consistent with payment network guidance to the marketplace, Chase has been developing the necessary technological capabilities to issue EMV-enabled credit cards across our portfolio, and expect that work to be completed by early 2015. Once that work is completed and validated, Chase plans to begin transitioning the credit card portfolio to EMV-enabled cards.

Debit Cards

There are two significant obstacles impeding Chase's transition to EMV-enabled debit cards. First, as you likely are aware, in July 2013 a Federal district court held that certain key elements of Federal Reserve Regulation II, which implements the Durbin Amendment to the Dodd-Frank Act and imposes in relevant part new requirements and restrictions related to network routing of debit card transactions, are invalid (*NACS v. Board of Governors of the Federal Reserve System*). The Federal Reserve has appealed this decision to the U.S. Court of Appeals for the D.C. Circuit. This litigation has created tremendous uncertainty as to what the applicable rules and standards will be. If the appellate court upholds the district court's findings, the Federal Reserve likely will revise Regulation II and could very well mandate that each debit card be enabled to support transactions on two signature networks, which simply is not possible today. Until the outcome of this litigation is clear and network routing rules are final, debit card issuers and networks cannot establish and promulgate definitive, Regulation II compliant EMV programming parameters, without which issuers are not in a position to produce EMV-enabled debit cards.

Second, current global EMV standards afford the cardholder the choice of which network the transaction will be routed over, if a card is enabled for more than one network. However, Regulation II takes an entirely different approach and provides that the merchant has the right to decide over which network the transaction will be routed. Solutions to this issue, providing for merchant routing of multiple unaffiliated networks on EMV-enabled cards utilizing a single EMV application exist, but there is not yet a common industry standard. Accordingly, both card issuers and merchants are reluctant to incur the significant but necessary development costs associated with transitioning to EMV-enabled debit cards until a definitive global industry standard is developed and adopted by all stakeholders.

Due to the uncertainty as to applicable network routing regulatory requirements created by the pending Regulation II litigation, as well as the lack of industry consensus on standards, Chase has not yet issued any EMV-enabled debit cards nor finalized a timeframe for enabling EMV on debit cards. We currently estimate that we will begin issuing EMV-enabled debit cards in 2015, assuming the Regulation II litigation is resolved and uniform standards are adopted by mid-2014.

Merchant Services

Chase Paymentech, our merchant acquiring business (“Paymentech”) has been deploying EMV-enabled point-of-sale devices since April 2012, when it began fully supporting EMV for Visa, MasterCard and American Express cards. In addition, Paymentech has been fully supporting EMV for Discover cards since 2013. Since 2012, Paymentech has processed over 180,000 EMV credit transactions, representing \$24 million in transaction volume.

Paymentech also has deployed many point-of-sale devices that are EMV capable but not yet enabled, and work is underway to get those devices certified to accept EMV transactions. However, the Regulation II issues referenced above must be resolved before full implementation can occur with respect to debit transactions.

2. When will all cards issued by your institution be EMV cards or include similar security features?

As stated above, Chase has been developing the necessary technological capabilities to issue EMV-enabled credit cards across our portfolio, and expect that work to be completed by early 2015. Once that work is completed and validated, we plan to begin transitioning the credit card portfolio to EMV-enabled cards as current cards expire at the end of their normal three-year reissue cycle. Following that timeline, Chase expects most of our credit card portfolio to be EMV cards by the end of 2017.

With respect to debit cards, once industry standards are adopted and Chase completes necessary technological development, Chase would begin issuing EMV-enabled debit cards for new cards issued from that point forward and would issue EMV-enabled replacement debit cards to current cardholders as current cards expire at the end of their normal three-year reissue cycle. Accordingly, if we are able to begin implementation in early 2015, the vast majority of our 34 million debit card portfolio would be EMV-enabled by the end of 2017.

3. What incentives do you provide to consumers, retailers, and financial institutions to encourage data security and the use of more secure cards? Have these been effective?

Chase provides a robust suite of digital alerts to consumers to notify them of “out of pattern” activities that may indicate their credit card or debit card information has been compromised.

These alerts have been effective at identifying fraudulent activity earlier and, therefore, reducing fraud losses.

Chase has made significant investments in authentication capabilities to prevent criminals from gaining access to consumers' credit and deposit accounts and information, including multi-factor authentication online and voice biometrics in call centers. In addition, we have made large scale investments in technology to identify "out of pattern" activity.

In addition, beginning in October 2015 the payment networks will shift liability for certain fraudulent transactions to the party with the least secure system. This will be an incentive, particularly for large retailers, to adopt EMV technology as doing so will insulate them from liability, as between retailers and card issuers, for fraud chargebacks resulting from counterfeit or lost/stolen cards.

For some time Paymentech has provided, for no charge, fully EMV capable/enabled "Future Proof" terminals to merchants newly enrolling with Paymentech through Chase branches. Paymentech also provides incentives to its existing merchants that upgrade to the Future Proof terminal. Paymentech also offers additional data security products – incorporating end-to-end encryption and tokenization– to its merchants for a fee.

4. Could you expedite the transition process to EMV cards? What would the costs and benefits be to doing so?

Chase could accelerate the re-issuance of our existing credit and debit cards, and thereby expedite the transition to EMV. However, there are a number of contingencies to delivering this acceleration, including concerns about the supply of chips in the market – especially if all issuers are trying to accelerate their transition. Moreover, the additional security EMV cards offer is contingent on merchant adoption of EMV card acceptance. Without merchant adoption, there is no added security – just the transition of liability for fraud losses beginning in October 2015 as noted above. Other activities, including enhanced cyber security efforts, issuer and merchant employee training and consumer education, will be necessary.

In addition, with respect to debit cards, there is the added challenge of ATM enablement as most debit cards also function as the customer's ATM card. There are approximately 450,000 ATMs in the United States operated by a wide array of banks and non-financial entities. Chase, which maintains the largest U.S. ATM network at present, only owns or has branded 19,500 of these machines. Similar to merchants, until all ATMs are enabled to accept and process EMV cards, much of the additional security EMV technology affords will not be realized.

Chase has several initiatives underway to make our own ATM fleet EMV-capable, including hardware remediation and software certification. Most of Chase's ATM fleet will be EMV-capable by mid-2014. Chase is currently certifying Maestro (MasterCard's non-U.S. ATM brand) cross border ATM EMV card transactions for the April 2013 Maestro cross-border liability shift

and plans to enable Maestro cross-border transactions at most ATMs later in 2014. We are still planning certification for the other networks, which will correspond with future ATM EMV liability shift dates (currently October 2016 for all other MasterCard cards, and October 2017 for all Visa cards).

While the aggregate EMV migration costs are significant (e.g., Chase alone anticipates spending over \$500 million to move our entire credit card and debit card portfolios to EMV cards), we do not anticipate significant incremental additional costs for accelerating migration efforts, assuming there is sufficient chip supply, common industry standards are adopted and the Regulation II litigation is resolved.

Merchant adoption, as well as adoption by ATM owners and operators, is the key to expediting the EMV transition. The primary impediments to quick merchant adoption are the Regulation II network routing uncertainties described above and, of course, cost. Merchant costs include hardware, system development, and implementation. The benefits include a more secure means of authentication for retail point-of-sale transactions but, as discussed above, not card-not-present transactions. Similarly, the primary impediment to quick ATM adoption is the lack of a common industry solution to support existing ATM network routing rules.

5. What other improvements are you pursuing to protect consumer data and prevent fraud?

Based on trends observed in other countries following EMV adoption, we expect criminals to change their focus to perpetrating fraud in channels where the card is not present (e.g., internet and telephone orders). Since EMV technology does not prevent fraud in these card-not-present channels, Chase is pursuing opportunities to (a) increase the amount of information merchants provide to card issuers for each card-not-present transaction such as the consumer's history with the device being used for the purchase and contents of the shopping basket and (b) leverage additional technology solutions to authenticate the person attempting a transaction. Chase is also working on developing tokenization capabilities, as mentioned above.

Chase has also implemented robust programs to protect consumer data, and to prevent and detect fraud. Chase operates an extensive cyber security and incident response program to secure our infrastructure and data in alignment with regulatory and industry standards, and to monitor and respond to existing and emerging threats. Our IT risk management function helps ensure Chase is responsive to information technology and systems risks. Chase's Global Security and Investigations group provides sophisticated fraud detection insight which enables Chase to identify early indicators of potential fraud. These programs and practices have enabled faster mitigation efforts and notification capabilities, and enhanced protection for our customers. Finally, Chase operates a privacy program to protect consumers and their data. All of Chase's security and privacy programs are subject to regulatory requirements and oversight.

6. What are the main impediments to the adoption of EMV cards and other security improvements?

As discussed above, the main impediments to adoption of EMV cards and other security improvements are (a) merchant acceptance of EMV cards, (b) the Regulation II issues and uncertainties, (c) costs, (d) supply of chips to support all payment cards outstanding, and (e) availability of technological and human resources necessary to meet marketplace and regulatory commitments.

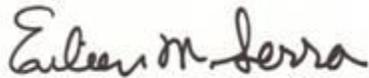
Adding EMV chips to debit and credit cards is part of a broader set of solutions necessary to enhance the U.S. payments systems' security. Even if every credit and debit card included an EMV chip today, retailers and other merchants, and ATM owners, must update their terminals and systems to accept EMV card transactions. But to do so, the marketplace needs clear and consistent rules to follow.

Moreover, the current solutions under discussion are designed to support multiple unaffiliated PIN point-of-sale networks only, which is consistent with current Regulation II. However, if the pending Regulation II litigation ultimately results in Regulation II being revised such that each debit card must be enabled for two unaffiliated signature networks, no industry solution yet exists. In any event, Chase is supportive of existing efforts to develop a common standard.

Chase agrees that the critical task of protecting Americans' consumer data is a shared responsibility, and we appreciate your recognition of our efforts in this regard. It is clear that financial institutions, payment networks, merchant acquirers, retailers, ATM owners, bank regulators and other government officials must work together to help ensure U.S. payment systems are as secure, convenient and reliable as possible. As discussed, this is a very complex topic with multiple stakeholders, numerous considerations and no single approach that readily works for all parties. Accordingly, Chase will continue our efforts and we look forward to further discussions and helping to develop collaborative solutions.

Thank you for the opportunity to respond to your inquiries and to contribute to this very important dialogue. If you have additional questions or would like to discuss in more detail, please ask your staff to contact Jason Rosenberg, Director of Federal Government Relations, at 202-585-6320 or at jason.m.rosenberg@jpmchase.com.

Sincerely,



Eileen Serra
CEO, Chase Card Services
Consumer & Community Banking



Mike Passilla
CEO, Merchant Services
Consumer & Community Banking



Barry Sommers
CEO, Consumer Bank
Consumer & Community Banking

Chris A. McWilton
President
North American Markets

MasterCard Worldwide
2000 Purchase Street
Purchase, NY 10577-2509

tel 1-914-249-5024
fax 1-914-249-4219
chris_mcwilton@mastercard.com
www.mastercard.com



February 5, 2014

The Honorable Al Franken
309 Hart Senate Office Building
Washington, DC 20510

Dear Senator Franken:

I write in response to your January 15, 2014 letter to Ajay Banga regarding the vitally important issue of payment card data security in the United States.

Payment technology is changing, transforming the consumer purchasing experience. As you noted in your letter, a key development in this evolution is the migration to EMV technology, which uses a microprocessor chip embedded in a payment card (rather than a magnetic stripe) to store cardholder data in a dynamic format that resists fraud and makes the production of counterfeit cards significantly more difficult.

This migration is about an upgrade that will drive both innovation and security for merchants, issuers and acquirers and, more importantly, consumers and cardholders. In addition, it will provide consumers a product that works consistently in virtually every market across the globe.

However, there is no "silver bullet" that addresses all payment card data security issues. We have invested, and we continue to invest, significant resources toward insuring that payment card transactions are safe and secure. We operate fraud prevention systems to protect data and prevent fraudulent transactions on 24/7/365 basis, and that effort, together with the efforts of others, has caused fraud levels to decline to all-time low levels.

Criminals and fraudsters will always try to steal from consumers and corporations. Our job is protecting consumers and businesses against these threats when they use payment cards. Of course, no financial transaction can be completely free from the risk of fraud. But, the implementation of EMV technology will serve as another layer of protection against the ongoing efforts of hackers and other criminals to compromise payment card data security.

Responses to your specific questions follow:

1. What is the status of your transition to the EMV technology?

MasterCard, along with Europay and Visa, created the EMV standard 15 years ago. That technology is managed today by EMVCo, an independent standards organization that continues to evolve a globally consistent approach to security to meet the evolving needs of consumers, merchants and issuers. EMVCo also has multiple levels of participation that establish an

invaluable mechanism for key industry stakeholders to provide input to EMVCo's Board of Managers, Executive Committee, and Working Groups. A range of organizations—including payment systems, networks, banks, processors, vendors, and more—contribute expertise.

Since the introduction of EMV, we have driven the implementation of the standard in markets across the globe, allowing for higher levels of security and global interoperability in payments. Today, MasterCard processes a significant volume of EMV transactions globally, including for customers in the U.S.

We introduced our future of payments “roadmap” for the United States in January 2012. In this roadmap, we took insights and perspectives from issuers, merchants and acquirers to outline an approach to enable the next generation of payments. Leading this roadmap is the belief that EMV is not about a specific device or cardholder verification method; it's about an overall approach to maximize the consumer payment experience and manage fraud into the future. It reflects our commitment to secure all payment channels including face-to-face, ATM, online and digital payments.

The roadmap does not mandate specific actions by merchants and issuers. Instead, it provides a path to help them make their own business decisions. A central element is the liability shift, designed as an incentive to help merchants and issuers move toward the EMV standard. In this liability shift, the party that employs the less secure technology will be liable for the potential fraud.

We are taking steps to incentivize the use of the most secure verification methods and reward the payment system participants who invest in the most secure methodologies. Today, that is PIN. But we have built flexibility into our hierarchies so they can adapt and change as new payment technologies and cardholder verification methods, such as biometrics, are created.

Over the past two years, we have been impressed with how the industry has come together to prepare and plan for this migration. We have seen, and continue to see, issuers and retailers move purposefully toward EMV. Issuers have begun providing cardholders with EMV cards as part of the normal card reissuance cycle (which usually takes place every three years for a card). Retailers have begun the process of installing EMV-compliant point-of-sale terminals, and many already have terminals in place and have begun the process of software enablement. Terminal manufacturers now only sell “world terminals,” which accept both magnetic stripe and EMV chip payments.

Based on our experience in other markets and industry research on merchant readiness plans, we expect that approximately 50 percent of merchant terminals will be EMV-compliant by October 2015. Furthermore, since high-traffic merchants are more likely to enable EMV terminals first, we expect that more than 50 percent of all card *transactions* will use EMV technology by October 2015. MasterCard will begin to make available more detailed projections for levels of card and terminal enablement in the coming months.

2. When will all issuers and acquirers on your network be required to issue and/or process EMV cards?

Acquirers processing MasterCard transactions have been required to have the capability to process EMV transactions since April 2013. We believe that issuers have strong incentives to issue EMV cards. However, there is no specific timeline over which issuers will be required to issue EMV cards.

Under the liability shift, issuers that do not issue EMV cards will bear a higher proportion of the risk for fraud arising from magnetic stripe cards. The purpose of the liability shifts that MasterCard has introduced is to drive coordinated migration, and to remove fraud from the system, rather than shifting liability *per se*. Our experience in other markets has shown that limiting liability for participants with the highest level of security provides a strong incentive for all participants to become fully compliant, which in turn adds security for everybody in the payment system.

Issuers that do not issue EMV cards will find themselves losing business to EMV issuers, particularly with respect to cross-border transactions. Many retailers in EMV-mature countries are now refusing to accept non-EMV cards, and we expect that the number of EMV-only retailers will continue to grow, particularly overseas. Issuers with customers who travel extensively will face significant pressure to make EMV cards available, or lose access to a significant portion of their clientele. As EMV technology is increasingly adopted by U.S. retailers, we expect that the market pressure on issuers to become fully EMV-compliant will only increase.

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?

As an initial matter, we believe that consumers should not be required to bear the risk of fraud, especially when that fraud risk is increased because parties have not adopted state-of-the-art technology like EMV chip technology. Accordingly, we offer consumer protections for unauthorized transactions greater than those required by federal law. MasterCard's Zero Liability Guarantee ensures that in most cases consumers will have no liability for unauthorized or fraudulent transactions on their credit cards or debit cards. The Zero Liability Guarantee is funded by issuers, reinforcing the commitment of MasterCard and our issuers to consumer peace of mind.

Nonetheless, consumers have already increased demands for secure EMV technology, driven in part because of the cross-border acceptance issue noted above, as well as the desire for increased security. As awareness of the benefits of EMV technology increases, consumer demand will increase accordingly.

With respect to retailers, our previously-announced EMV roadmap provides strong incentives for retailers to move to the EMV standard:

- October 2012: We began to offer audit relief under the Payment Card Industry Data Security Standard (“PCI DSS”) to retailers that have implemented EMV terminals and process a specific percentage of transactions via these terminals (although compliance with PCI DSS is still, of course, required).
- October 2013: We began to offer merchants real financial relief as they take steps to reduce their exposure to Account Data Compromise (“ADC”) liabilities, even as they continue to invest in PCI audits. MasterCard will offer up to 50 percent ADC liability relief to a merchant when more than 75 percent of the MasterCard transactions from that merchant originate from an EMV contact and EMV contactless terminal.
- October 2015: We will increase the extent of our liability relief to 100 percent to merchants when more than 95 percent of their transactions originate from an EMV contact and EMV contactless terminal. At the same time, we will implement new “liability hierarchies” for all point-of-sale transactions other than automated fuel dispensers. These liability hierarchies will provide that the party in a transaction that does not implement the highest level of security bears the risk of fraud loss with respect to that transaction.
- October 2016: The new liability hierarchy will take effect for all U.S. ATM transactions.
- October 2017: The new liability hierarchy will take effect for automated fuel dispensers.

We believe that these rule changes will provide a strong incentive for both retailers and issuers to implement EMV technology, while ensuring that entities that make the investment in EMV do not suffer losses because of non-EMV-compliant participants. The gradual introduction of these programs gives merchants, acquirers and issuers concurrent incentives to implement the highest levels of security as they become available. Our experience in other markets has shown that providing incentives for all participants in the MasterCard system to implement EMV technology is the best way to drive coordinated implementation across all sectors.

4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?

Moving a payments system as large and complex as the United States payment system does not happen overnight. We have the largest market for payment cards in the world, with thousands of financial institutions issuing domestic cards and acquiring domestic transactions, and millions of point-of-sale terminals that must be upgraded to accept EMV transactions.

Other markets demonstrated a higher need for EMV technology at an earlier time, due in part to poorer telecommunications systems, higher historical fraud levels, or both. In turn, the lessons learned by implementing EMV in other jurisdictions have informed our efforts at U.S. implementation.

Today in the United States, the work of migration is well underway. Since we issued our EMV roadmap in 2012, the industry has made significant progress in EMV implementation. We helped bring the industry—merchants, issuers, acquirers, manufacturers and others—together to coordinate the migration to EMV. This activity is facilitated by the U.S. EMV Migration Forum, an independent, cross-industry body that addresses issues requiring broad cooperation and coordination across many constituents in the payments space to promote the efficient, timely, and effective migration to EMV-enabled cards, devices, and terminals in the United States.

Merchants and issuers alike have prepared their plans based on the dates in our and other networks' roadmaps. I reemphasized in a letter to our customers and partners on January 8, 2014 our belief that now is the time to migrate to EMV in the U.S. We will not delay our implementation timeline, as there is too much at stake to stop the current progress in payment technology and security.

5. What other improvements are you pursuing to protect consumer data and prevent fraud?

EMV, while a highly important step in ensuring payment security, is not a comprehensive solution to data security and fraud prevention. Hackers and other criminals are constantly searching for weaknesses in the payment system, and participants in the payment system must use multi-layered, adaptable security approaches to stay ahead of bad actors to the greatest extent possible.

We are constantly working to improve security on our network. For example, we offer state-of-the-art fraud monitoring services to our customers that identify fraud patterns both domestically and internationally, and alert issuers and acquirers to unusual activity patterns. These services increase the ability of our customers and partners to minimize the impact of hacking and other data theft when it does occur. We are committed to continuous improvement of our fraud detection and prevention capabilities. Much of our investment in data security and fraud prevention is for the benefit of others in the payments industry that may not invest at nearly the same level as MasterCard does. We understand and embrace our role as an industry leader in this regard, and will continue to invest significant resources in keeping up with constantly-evolving security threats.

Another key component in payment data protection and fraud prevention is the PCI DSS, which is a set of data security standards promulgated by the Payment Card Industry Security Standards Council ("Council"). The Council's mission is to enhance payment card data security by developing and maintaining appropriate security standards and related tools, and driving education and awareness of the critical importance of data security. The Council publishes these standards for anyone to access but specifically for the payment card industry's use in security and compliance programs. The PCI DSS are constantly being evaluated and upgraded to enhance security.

We are also working to enhance security for online transactions, which constitute an ever-growing proportion of consumer transactions. In October, we, along with Visa and American Express, introduced a proposed framework for a new global standard to enhance the security of digital payments, using secure "tokens" (rather than payment card numbers) to

process online transactions. Using tokens for online payments will, similar to EMV chip technology, drastically reduce the utility of stolen information to hackers and criminals.

We are introducing other technologies to further secure online payments. For example, handheld card readers can bring the security features of EMV to online transactions. Also, MasterCard's SecureCode is a private code shared only between a consumer and an issuer, which allows confirmation directly between the consumer and issuer that the card is being used by an authorized user.

6. What are the main impediments to the adoption of EMV cards and other security improvements?

The U.S. payments market is both larger and more complex than any other market in the world. Therefore, coordination among issuers, acquirers and retailers will take longer than in smaller markets. This has, no doubt, contributed to the delay in EMV implementation, and presents challenges toward the implementation of any security improvement that requires widespread modifications to technology, procedures or both.

Additionally, EMV implementation is not a cost-free exercise. However, MasterCard has a proven commitment to lowering the burden of EMV compliance. Our EMV implementation roadmap has provided issuers, acquirers and retailers the flexibility to manage their business and technology decisions, particularly with respect to EMV. To aid payment system participants in their EMV adoption process, we have introduced a streamlined testing and certification process.

Finally, the recent court rulings on implementation of the Durbin Amendment have created uncertainty in the market, and have caused some participants to hesitate in allocating important resources to EMV implementation. None of us can ignore the possibility of future changes to U.S. debit routing requirements. While the landscape may look differently in months or years, we cannot stop progress on EMV implementation because there is too much at stake for all of our customers.

We introduced the first U.S. EMV solution to enable the routing of PIN debit transactions over multiple, unaffiliated networks, and decided to license that technology to other networks for free. That technology continues to be open to all—at no cost—and is helping our customers to implement EMV within the requirements of the Durbin Amendment's non-exclusivity provisions.

In short, MasterCard has invested significant resources in bringing EMV to market while minimizing the burden on payment system participants to the extent possible. We are committed to doing the same with respect to security improvements in the future.

EMV is a critical upgrade to the U.S. payment system, and recent retailer data breaches demonstrate that the cost of additional security breaches is much greater than the cost of upgrading to EMV and implementing new security improvements as they are developed. However, we must ensure that the drive to migrate to EMV technology does not lose momentum when these recent security breaches are no longer in the media spotlight. MasterCard remains committed to continuing to drive EMV implementation, and we hope that broader support for that implementation process is the silver lining from these costly data breaches.

* * *

MasterCard appreciates the opportunity to respond to your questions regarding EMV technology and payment data security. I hope you and your staff will continue to look to MasterCard as a resource. Tucker Foote heads our government affairs office in Washington, D.C., and he can be reached at 202-414-8014 or tucker_foote@mastercard.com. Of course, please feel free to reach out to me directly if you have any follow-up questions or if I can be of assistance to you in any way.

Sincerely,

A handwritten signature in black ink, appearing to read "Chris McWilton", with a long horizontal flourish extending to the right.

Chris McWilton
President, North American Markets
MasterCard



February 5, 2014

Ellen Richey
Chief Enterprise Risk Officer

The Honorable Al Franken
Chairman
Senate Judiciary Subcommittee on Privacy,
Technology and the Law
309 Hart Senate Building
United States Senate
Washington, DC 20510

Dear Senator Franken,

Thank you for your January 15, 2014 letter regarding the importance of protecting Americans' personal information. As we have seen in recent breaches, whether it's information related to payment cards or personally identifiable information contained in customer databases, cyber criminals will seek to infiltrate any vulnerability to access this data. When they are successful, criminals steal more than money; they steal peace of mind. At Visa, nothing is more important than trust in the payment system.

For more than 50 years, across the globe Visa has enabled people, businesses and governments to make and receive payments efficiently and securely. As a result of the industry's security investments, we've seen fraud rates decline by more than two-thirds over the past two decades. Our collective success in maintaining the trust and confidence of consumers comes from an ability to work together, share information and coordinate our defenses.

Visa believes the protection of consumer data is the shared responsibility of all parties, including payment networks, financial institutions and merchants. The industry secures payment card data through a layered approach because no single solution can eradicate fraud. It takes the combination of technology, processes and people to guard account information from enterprising and well-funded cyber criminals.

At Visa, we continually invest in a number of measures to protect and devalue information. Some of these security measures include end-to-end encryption, tokenization and risk-based authentication among others. We also deploy technologies to help identify and prevent fraud. One such technology investment is a service that provides an instantaneous rating of a transaction's potential for fraud to the financial institution that issued the card, including whether it was part of a reported data security compromise. This rating occurs as part of the transaction authorization and enables the issuer to make a more informed decision about whether to accept or decline the transaction, based, in part, on this sophisticated evaluation. Our advanced fraud analytics are unique to the U.S. and have helped to identify and prevent billions of dollars of fraud.

It is important to highlight that, when fraud does occur, consumers are always shielded from liability for unauthorized Visa purchases. Visa and our financial institution partners have a zero liability policy for consumer credit and debit cards – protection that goes beyond what's required by Federal law and exceeds the protection offered by some other payment solutions including certain ACH or PIN debit networks.

Page 2

But our work is never done. Keeping pace with criminals will always require the investments of many aligned toward a common purpose. We are committed to working collaboratively with financial institutions and merchants to foster a secure payments environment, including promoting the adoption of EMV as part of the industry's approach to safeguarding payment card data in the United States.

Below are the responses to the important questions you raised. Thank you for the opportunity to share this information.

Sincerely,

A handwritten signature in blue ink that reads "Ellen Richey". The signature is written in a cursive style with a large, looping initial "E".

Ellen Richey

1) What is the status of your transition to the EMV technology?

Visa supports the adoption of EMV technology in the United States. We view EMV as an important piece of a multilayered approach to security that introduces dynamic authentication for the face-to-face, card-present environment and helps mitigate counterfeit fraud. If stolen, dynamic data is less valuable to criminals, making our nation's retailers less of a mark for hackers.

We think it is important for the payments system to move to dynamic authentication; but as we have seen in other parts of the world, it requires the support of all parties involved – merchants, financial institutions, processors and the networks.

Globally, other markets originally adopted EMV chip because expensive telecommunications infrastructure prohibited their ability to conduct real-time network authorizations as occurs on virtually all transactions in the United States. As a result, a technology was needed that conducted security checks between the card and terminal; thus the emergence of a microchip. Today, there are 1.6 billion active EMV chip cards used for credit and debit payments at 15.4 million EMV acceptance terminals deployed around the world. Globally, 36 percent of cards in market and 65 percent of terminals in stores are based on the EMV standards.¹

While the United States has had success in managing fraud using sophisticated technology to conduct security checks behind the scenes and through significant investments to secure account data wherever it resides, we recognized the need to do more. That's why in August 2011, Visa announced a series of initiatives to accelerate the migration to EMV chip technology in the United States as outlined in response to your second question below. Visa's roadmap supports a variety of cardholder verification methods, including signature, PIN and no authentication, to accommodate the various different environments that payment cards are accepted in today.

It is important to recognize EMV is but one piece of a comprehensive approach to data security and is not a solution to all challenges, especially Internet shopping and other card-not-present environments. Visa has worked with financial institutions and the merchant community as we have developed our timeline for implementing EMV, and we are committed to continued collaboration with industry partners in support of the transition.

2) When will all issuers and acquirers on your network be required to issue and/or process EMV cards?

Visa's EMV roadmap does not mandate the adoption of chip, but instead provides important marketplace incentives to encourage adoption by Visa financial institutions and merchants. As part of our incentive program, we put in place a liability shift that makes the party that has not deployed EMV capabilities responsible for any resulting counterfeit fraud, effective October 1, 2015 (for most point-of-sale environments), and October 1, 2017 (for Automated Fuel Dispensers and ATMs, which are more complicated and expensive terminals to replace). As an additional step toward EMV readiness, last year Visa worked with all U.S. Visa acquirer endpoints to ensure they are capable of supporting merchant acceptance of EMV chip transactions. As a result, acquirers representing 95 percent of Visa's payment volume have been certified to support EMV chip processing. This is a key milestone in the EMV implementation process.

It is important to recognize that the investment required by merchants, acquirers and issuers is substantial. Often, investments such as these are easier for larger stakeholders than smaller

ones, and we are mindful to allow enough time for this change to occur without disadvantaging smaller merchants or issuers, or disrupting the ability for consumers to transact as these conversions occur.

3) What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?

As part of the EMV migration roadmap, Visa has instituted a U.S. liability shift for domestic and cross-border counterfeit card-present point-of-sale (POS) transactions, effective October 1, 2015. Fuel-selling merchants and ATMs will have an additional two years, until October 1, 2017, before a liability shift takes effect, given their more complex terminal environments. Currently, counterfeit fraud in the face-to-face, card-present environment is typically absorbed by card issuers, with partial reimbursement in some cases where a breached entity is found not to be compliant with the PCI Data Security Standards. With the liability shift, if a contact chip card is presented to a merchant that has not deployed, at minimum, a contact chip terminal, liability for counterfeit fraud will shift to the merchant's acquirer. It is typical for the merchant acquirer to pass the fraud expense on to the merchant. If a magnetic stripe only card is presented to a merchant who has deployed a contact chip card terminal, the issuer will bear the liability for the counterfeit fraud. The liability shift encourages chip adoption and reduces fraud because any chip-on-chip transaction (chip card read by a chip terminal) provides the dynamic authentication data that effectively mitigates counterfeit fraud. Experience from many countries has shown that liability shifts are the single most effective tool for moving markets to migrate from magnetic stripe environments to EMV chip.

4) Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?

The four-year timeline that Visa originally established in 2011 is actually quite aggressive considering the timelines we have seen in other markets. Further expediting this timeline would present additional challenges given the complexities of the payments ecosystem. There are thousands of market participants who need to make the appropriate and necessary investments in infrastructure and systems. Factors such as length of card and terminal lifecycles are critical factors in the time it will take to issue new EMV cards, replace terminals and integrate software into complex merchant point-of-sale environments. As stated earlier, we are mindful of key considerations including: ensuring a level playing field amongst stakeholders of all sizes, the potential costs to industry participants of transitioning millions of cards and millions of terminals to a new type of payments technology, and of implementing requirements in a way that will facilitate and encourage the growth of commerce.

Visa is committed to working with issuers, acquirers, merchants, and others in the payments ecosystem as they migrate to EMV. We believe the roadmap we have established will effectively facilitate the transition in a timely manner.

5) What other improvements are you pursuing to protect consumer data and prevent fraud?

Visa recently announced, along with MasterCard and American Express, a proposal to create a new global industry security standard for payment tokenization. Replacing the traditional account number with a digital payment "token" for online and mobile transactions eliminates the need for the merchant, digital wallet operators or others to store (or protect) primary account numbers. Payment tokenization provides added benefits of restricting the token's use to the domain (or

merchant) for which it was requested. This tokenization standard was developed to take advantage of EMV's dynamic authentication, bringing elements of the same investments that are being made for EMV chip card technology to the mobile and eCommerce payment environments.

Visa is committed to enhancing security measures that adjust to the evolving landscape and promote innovative approaches to payments, while mitigating and preventing fraud. Tokenization is one component in this multilayered approach, which also includes a number of other measures such as Visa Advanced Authorization, the Visa Consumer Authentication Service, Verified by Visa, and end-to-end encryption services available in the market today. In addition, Visa works closely with merchants and financial institutions on network security to help prevent fraud, protect consumer information and respond quickly when there has been a data compromise.

6) What are the main impediments to the adoption of EMV cards and other security improvements?

Given the diverse payments ecosystem that exists in the U.S., there are a number of factors which impact any broad industry change, most notably cost to reissue cards and replace retailer terminals. There are thousands of market participants, including issuers, issuer processors, acquirers, acquirer processors, and merchants, each with varying degrees of sophistication, their own business objectives, financial drivers, and an evolving marketplace. Migrating this many stakeholders, while maintaining the reliability of the payment system that hundreds of millions of people have come to rely on, takes a significant investment in time, money and resources. Further, there are challenges to speeding implementation including the legal uncertainty associated with recent debit card regulation. Lack of clarity on the routing requirement and pricing for debit cards makes it difficult to ensure solutions and investments will be compliant with the law.

Some industry groups are using recent data compromises to suggest that PIN for all payment transactions would be a safer alternative. Visa's priority is to ensure that the use of static data such as PINs is steadily reduced in payments, particularly where more robust and dynamic technologies, EMV as an example, are available for protecting data. Indeed, PINs are particularly sensitive, as a compromise of PIN data could allow criminals to directly access funds in checking accounts or credit cards through ATMs. Mandating specific forms of customer authentication will also delay adoption and increase the cost of migrating to EMV, since the vast majority of merchants in the United States have chosen not to install the infrastructure necessary to accept PIN transactions, nor do they have the system capabilities to protect PIN data. Taking a "one size fits all" approach of requiring PIN for all chip transactions would inhibit payment methods and acceptance where PIN usage is not feasible, for example, "wave and go," as well as new and innovative payment devices using mobile or other technology.

Visa has worked to put in place a roadmap to help facilitate this transition and provide incentives for these investments so all participants can plan and implement the transition to EMV. Visa continues to engage with financial institutions, merchants and others in the payments system to ensure the Visa network and its endpoints are enabled to support the migration to EMV chip technology.

ⁱ EMVCo LLC



February 5, 2014

Chairman Al Franken
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Franken:

In light of recent merchant breaches, we appreciate your interest in the safety and security of the payments system in our country and the opportunity to highlight our mutual interest in this topic. For more than 160 years, account security has been a top priority for Wells Fargo. Today, we remain as committed as ever and use proven technologies to protect our customers' financial information and privacy.

We continually work to further strengthen our fraud prevention measures, including – but not limited to – taking demonstrable steps toward offering, when appropriate, products with EMV technology. Along with a number of other technologies and security measures that are being used or developed by card issuers, EMV can help make transactions more secure in a “card present” situation. For “card not present” situations, like mobile and online payments, we continue working to ensure the safety and security of customer information. Further, we will continue collaborating with our industry colleagues in the payments system (card networks, merchants and issuing colleagues) to develop industry standards to help protect consumers.

1. *What is the status of your institution's transition to EMV cards?*

First, it is important to note that today, very few domestic merchant terminals support EMV technology, so any EMV cards issued have limited merchant acceptance in the United States. As merchant chip card acceptance gains popularity in the U.S., we will evaluate the best way to support our customers' credit card and debit card needs in advance of the networks' mandated fraud liability shift scheduled for October 2015. The general principle behind the shift is that if the merchant has EMV capability and the card does not contain the EMV chip, the issuer will incur the fraud loss. Likewise, if the card has the EMV chip, but the merchant does not have EMV equipment, the merchant will incur the loss.

For customers who travel to countries where EMV technology is more prevalent, we offer Visa-branded consumer credit cards enabled with EMV technology upon request. If a new card is requested, it will be equipped with chip-based and contactless technology, as well as a magnetic stripe. That means Wells Fargo Visa consumer credit cardholders can use the card at any kind of terminal they may encounter.

For our Wells Fargo debit card customers, we are in the process of completing EMV technical development. Our initial plan is to make these cards available to customers that travel internationally. This development has been slowed in part as a result of the ruling in the *NACS v Board of Governors of the Federal Reserve System* case, which suggested that each type of authorization method, both signature and PIN, required two unaffiliated network routing options. This ruling, which is on appeal, has created uncertainty as to network routing requirements and presents an obstacle to EMV implementation for debit cards. If the existing Regulation II routing rules issued by the Federal Reserve Board stand as is, there are options in place to support those requirements.

2. *When will all cards issued by your institution be EMV cards or include similar security features?*

As the fraud landscape evolves, we adapt our approach to fighting fraud and counteract new threats by using innovative tools and technology to help keep customer information safe. To that end, EMV and other proven fraud prevention strategies will always be in our fraud fighting toolkit. Though we do not currently have a date by which all cards will have an EMV chip, factors such as the fraud liability shift announced by Visa (scheduled for Oct. 2015) and the outcome of the *NACS v. FRB* case will heavily influence the timing of the payments system's widespread adoption of this technology.

3. *What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?*

We believe the payment networks (Visa, MasterCard, and American Express), not issuers are best positioned to speak to the topic of incentivizing EMV adoption.

Generally speaking, a secure payments system is in everyone's best interest. Perhaps the strongest encouragement is Visa's announcement that a counterfeit fraud liability shift would occur beginning October 2015. As a financial institution, we are committed to working with colleagues in the payments system to ensure any potential fraud-prevention technology – including EMV – is explored and used to its best potential to help protect consumers.

4. *Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?*

We have the technical capability to issue debit and credit cards with EMV technology and, depending on our vendors' capacity, we could likely issue at a faster pace. However, there are several important points to consider:

- a. Consumer education of EMV utilization will need to be done in phases so merchants and financial institutions can ensure a smooth transition.

- b. Because it takes an EMV card and an EMV point of sale terminal in order to leverage EMV technology, faster card issuance will not provide cardholders with a significant increase in security until such time as merchants have also upgraded their card acceptance equipment to be EMV compliant. As we have noted, very few domestic merchant terminals currently support EMV technology.
- c. A fully functional and vibrant EMV payments system provides limited fraud protection in “card not present” transactions such as those conducted online.

5. *What other improvements are you pursuing to protect consumer data and prevent fraud?*

The safety and security of our customers’ sensitive financial information is our top priority and for that reason, as a regular course of business, we look for ways to protect it. In fact, our regulator, the Office of the Comptroller of the Currency, examines us to ensure we are taking reasonable precautions to safeguard customer data and customer privacy.

It is also important to point out that preventing counterfeit card fraud only represents one aspect of card security; we also work to protect cardholders against online fraud – a scenario not protected by EMV technology.

Whether or not emerging fraud prevention technology has been implemented, our cardholders are protected by Zero Liability. This means that if a Wells Fargo Credit Card or Debit Card is ever lost, stolen or used without cardholder authorization and the cardholder provides us with prompt notification, the cardholder is protected against any unauthorized transactions made at merchants, over the phone, on the Internet or at an ATM.

6. *What are the main impediments to the adoption of EMV cards and other security improvements?*

As noted earlier, very few domestic merchant terminals support EMV technology, so any EMV cards issued today would have limited merchant acceptance in the United States. As EMV card issuance becomes more prevalent, merchants will also need to upgrade to EMV capable point of sale terminals. As merchant chip card acceptance gains popularity in the U.S., we will evaluate the best way to support our customers’ credit card and debit card needs in advance of the fraud liability shift scheduled for October 2015.

Particularly in the debit card space, continued regulatory uncertainty – specifically the outcome of the *NACS vs. FRB* case – is an impediment. Another impediment is the fact that EMV technology only addresses fraud in “card present” situations. Separate solutions, and further investments, will be required to address fraud that occurs in a “card not present” situation.

We share your interest in a strong payments system that affords consumers and merchants the ability to make secure transactions both domestically and abroad. Wells Fargo takes the security of our customers’ data very seriously and is constantly evaluating potential threats and new technologies to combat those threats. We are committed to working to continually improve offerings, policies and procedures, while also providing our customers with the tools and information they need to support a safe and secure payment environment. Providing a

safe and secure environment for payments, whether at the point of sale, online, or in a mobile context, is a shared responsibility of merchants and the payments industry. The threats to safe and secure payments are constant and dynamic. To be effective, our fraud fighting tools also need to evolve and change, and no single technology can be the solution.

We appreciate the opportunity to respond to your inquiry and would welcome the opportunity to discuss with you or your staff.

Sincerely,

Handwritten signature of Beverly J. Anderson in black ink, featuring a stylized 'B' and 'A'.

Beverly J. Anderson
Executive Vice President
Consumer Financial Services

Handwritten signature of Edward M. Kadletz in black ink, featuring a stylized 'E' and 'K'.

Edward M. Kadletz
Executive Vice President
Head of Debit Card