Before the
FEDERAL RESERVE BOARD OF GOVERNORS
Washington, D.C.

In the Matter of	)	
	)	
Debit Card Interchange Fee and Routing	)	Docket No. R-1404
Interim Final Rule; Request for Comment	)	RIN 7100-AD63
	)	

COMMENTS OF
THE SECURE ID COALITION

The Secure ID Coalition (SIDC) hereby submits the following comments regarding the Board of Governors of the Federal Reserve System (Board) Interim Final Rule on Debit Card Interchange Fees and Routing.[1] The SIDC applauds the Board for looking into possible frameworks for adjusting interchange fees to incentivize fraud-prevention measures to safeguard consumers from credit and debit card theft and fraud. As explained below, the SIDC has great confidence that the Board will recognize how EMV/Chip-and-PIN fraud prevention technologies have become the *de facto* standard for securing payment cards worldwide, and will adopt Chip-and-PIN technology standards to the benefit of American consumers, as it is the prime technology approach most trusted to identify and prevent fraudulent transactions; monitor incidence, reimbursement and losses with respect to fraudulent transactions; respond appropriately to suspicious transactions (so as to limit losses and prevent fraudulent transactions); and secure debit card and cardholder data. We also believe that the EMV technology approach will be the least onerous approach for issuers, as it is used globally to great success by the world's four largest card issuers, American Express, JCB, MasterCard, and Visa.

---

[1] Debit Card Interchange Fees and Routing, 76 Fed. Reg. 43478 (2011).

INTRODUCTION

Founded in 2005, the Secure ID Coalition works with industry experts, public policy officials, and federal and state agency personnel to promote identity policy solutions that enable both security and privacy protections. Because of our commitment to citizen privacy rights and protections, we advocate for technology solutions that enable individuals to make their own decisions about the use of their own personal information. Members of the SIDC subscribe to principles that include the increased deployment of secure identity solutions, as well as advise on – and advocate for – strong consumer privacy protections and enhanced security to eliminate waste, fraud, theft, and abuse. The SIDC is headquartered in Washington, D.C.

The SIDC submits these comments on the Debit Card Interchange Fee and Routing Proceeding (Proceeding) so that the Board may develop a robust plan to best foster an environment where businesses and consumers may use their debit and credit cards both online and around the world safely. Consistent with the SIDC's previous comments in this proceeding, we strongly recommend the Board utilize a technology-specific approach that issuers must adopt in order to receive additional transactional compensation.

To achieve the maximum level of fraud prevention for the least amount of systemic cost – as well as to take advantage of existing economies of scale on a global basis – the SIDC specifically recommends utilizing the Europay/Mastercard/Visa (EMV)[2] framework successfully used world-wide for payment applications. Also known as 'Chip-and-PIN,' the EMV payment regime uses smartcards – secure integrated circuit chips in card form factor – as they are the globally accepted gold-standard of payment card fraud protection technology. We will discuss in detail how EMV technology will satisfy the four criteria laid out in the Proceeding.

---

[2] EMV is a global standard for credit and debit payment cards based on smartcard technology. Developed in 1999, the EMV standards are maintained and managed by EMVco, a limited liability corporation owned and operated equally by American Express, JCB, MasterCard and Visa. According to their website, www.EMVco.com, by end-2010, there were more than 1.24 billion EMV compliant chip-based payment cards in use worldwide.

DISCUSSION

A Technology-Specific Solution to Protect Consumers from Financial Fraud

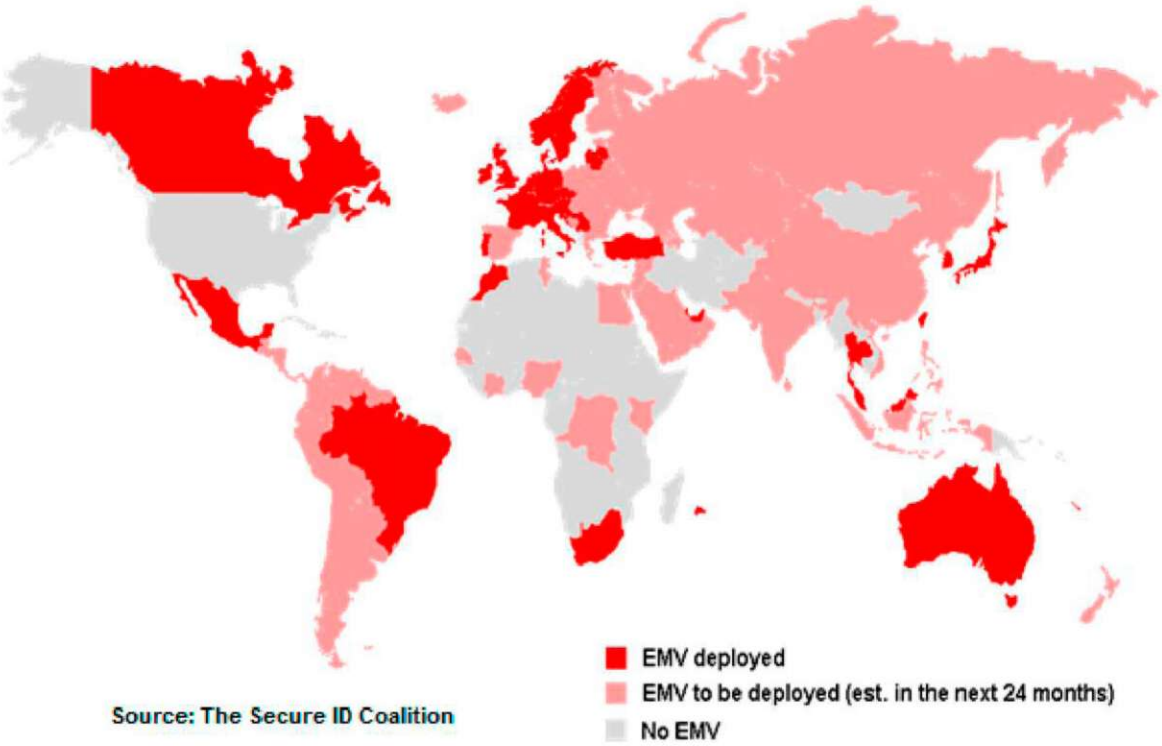
The SIDC supports a technology-specific solution to protect consumers from financial fraud – as opposed to a non-prescriptive standard – for a number of reasons. Up to now, financial institutions have long had the opportunity to implement fraud prevention measures in the US market; at their best, they have measured up to be fraud-appeasing, and at their worst, fraud-inducing. For instance, the federal Fair Credit Billing Act[3] limits the liability of card holders to $50 in the event of theft of the actual credit card, regardless of the amount charged on the card, if reported within 60 days of receiving the statement. Once successfully charged back to the financial institution, the financial institution then charges back the merchant, who is then forced to pass the costs back on to the consumer. Amounting to a never-ending shell-game, fraud is never *prevented,* it is only *passed back to the consumer.*

While the SIDC agrees that generally markets should be allowed to pick 'winners and losers', the SIDC strongly believes that the market *has* spoken, as evidenced by the global adoption of Chip-and-PIN as the global standard in financial card fraud prevention.

As evidenced by the chart on the next page, *almost* every G-8 and G-20 nation has adopted the Chip-and-PIN standard; we highlight 'almost,' as the only G-8/G-20 nation not to do so is the United States. In this, we have the dubious distinction of joining countries such as ***Afghanistan, Angola, Bangladesh, Cambodia, Eritrea, Ethiopia, Iran, Iraq, Libya, Liberia, Mozambique, Pakistan, Papua New Guinea, Rwanda, Somalia, Tajikistan and Turkmenistan*** where the financial payments industry is not interested in protecting its customers with secure card technologies.

[3] 15 U.S.C. § 1601 et seq.

Global Chip-and-PIN Adoption, by 2013



Source: The Secure ID Coalition

The following countries currently use CHIP-and-PIN for credit/debit transaction:

Armenia
+Australia
Austria
Belgium
+Brazil
+*Canada
Croatia
Czech Republic
Denmark
+*France
+*Germany
Ireland
+*Italy
+*Japan
Latvia
Lithuania
Malaysia
Mauritius
+Mexico
Morocco
Netherlands
Norway
Portugal
Serbia
Slovenia
+South Africa
+South Korea
Sweden
Switzerland
Taiwan
Thailand
+Turkey
UAE
+*UK

****G-8 Countries***
+G-20 Countries

The following countries by 2012 plan to deploy CHIP-and-PIN for credit/debit transaction:

+Argentina
Azerbaijan
Belarus
Belize
Bolivia
Bosnia and Herzegovina
Bulgaria
Cayenne
Chile

+China
Columbia
Costa Rica
Cote D'Ivoire
Ecuador
Egypt
El Salvador
Estonia
Finland
Georgia
Greece
Guatemala
Guyana
Honduras
Hungary
+India
+Indonesia
Israel
Jordan
Kazakhstan
Kenya
Kuwait
Macedonia
New Zealand
Nicaragua
Nigeria
North Korea
Oman
Panama
Paraguay
Peru
Philippines
Poland
+*Russia
+Saudi Arabia
Senegal
Slovakia
Spain
Sri Lanka
Suriname
Syria
Tunisia
Ukraine
Uruguay
Venezuela
Vietnam
Yemen
Zaire

The following countries do not have/nor plan CHIP and PIN deployments:

Afghanistan
Albania
Algeria
Angola
Bangladesh
Benin
Bhutan
Botswana
Burkina Faso
Burma
Burundi
Cambodia
Cameroon
Cape Verde
Central African Republic
Chad
Djibouti
Equatorial Guinea
Eritrea
Ethiopia
Gabon
Ghana
Guinea
Guinea-Bussan
Iran
Iraq
Kyrgyzstan
Lesotho
Liberia
Libya
Laos
Luxemburg
Madagascar
Malawi
Mali
Mauritania
Mongolia
Mozambique
Namibia
Nepal
Niger
Pakistan
Papua New Guinea
Republic of Congo
Rwanda
Sierra Leone
Soa Tome and Principe
Somalia
Sudan
Swaziland
Tajikistan
Tanzania
The Gambia
Togo
Turkmenistan
Uganda
+*United States
Western Sahara
Zambia
Zimbabwe

***G-8 Countries**
+ G-20 Countries

Subjective non-prescriptive standards are appropriate when there are multiple technologies that can more-or-less achieve the same goals when the market is still deciding on the best way to deliver a consumer benefit, such as home video recording (e.g., VHS vs. Beta), or personal computing platforms (e.g., Mac vs. PC). However, the Board faces a far more urgent situation – not only in deciding how to rein in rampant fraud both online and off that costs consumers billions of dollars a year, but in ensuring that US citizens will be able to transact business globally.

To that point, the European Payments Council[4] has announced their plans to allow merchants to *refuse magnetic stripe transactions altogether,* thus denying US travelers abroad the ability to use their current credit and debit cards, as well as mandating that all card-not-present transactions on both the issuing and acquiring side have an appropriate authentication solution by the end of 2013. When this goes into effect, US citizens using their current payment cards will be utterly unable to participate in card-not-present transactions with merchants across the European Union.

The Board noted in its previous NPRM that "the drawback of adopting technology-specific standards is the risk that it would cause issuers to under-invest in other innovative new technologies, not included in the Board's standards, that may be more effective and less costly than those identified in the standards."[5]

American consumers do not have the luxury to wait until *another* alternative standard is determined, nor should they when a proven, mature standard is already at hand that actually *prevents* fraud. By adopting the internationally accepted Chip-and-PIN standard, the Board may ensure that they will be taking advantage of a powerful network effect granted by Chip-and-PIN: in utilizing an *internationally tested, accepted, and mature method of securing financial cards*, they will ensure that US consumers will be able to take advantage of strong privacy, security and fraud prevention mechanisms *and* allow American citizens to continue financial transactions across the European Union, our largest economic trading partner.

---

[4] European Payments Council, *Resolution: Preventing Card Fraud in a Mature EMV Environment,* Doc. EPC424-10, 31 January 2011.

[5] Debit Card Interchange Fees and Routing, 75 Fed. Reg. 81742 (2010).

Chip-and-PIN Technology Discussed With Regard To The Interim Rule's Four Criteria

The SIDC recommends that issuers deploy EMV payment applications on smartcards that can be used by either inserting the card into a Point-of-Sale (POS) reader slot, or other form factors utilizing secure, integrated micro-controller chips that can be used by tapping the POS reader's contactless interface with the form factor. This approach will address the four criteria set forth in the rule covering traditional card payments, with the added benefit of also securing Internet payments for e-commerce, and mobile near-field communications (NFC) payments from a cellular handset or other mobile device.

The EMV approach will address the Board's four criteria in the following fashion:

Criteria 1: Identify and Prevent Fraudulent Transactions

- Where offline authorization support is required, the EMV technology's PIN capability substantially aids in protecting against lost and stolen card fraud.

- EMV technology is already utilized in the eCommerce and eBanking worlds globally. Card Authentication Program (CAP) and Dynamic Passcode Authentication programs defined by MasterCard and Visa allow for the fundamental principles of EMV deployed in the physical world to also be implemented in the virtual world. Hence, EMV can be utilized to help counteract card-not-present fraud as well. In eBanking, Further, EMV provides for two-factor authentication to be employed to help issuers protect against phishing attacks.

Criteria 2: Monitor Incidence, Reimbursement and Losses With Respect To Fraudulent Transactions

- Because the EMV standards utilize smartcards and mobile NFC, they are able to authenticate the holder of the card using the chip's on-board computer without having to access a central database located elsewhere. This means that a transaction can be authorized without needing an Internet connection, allowing the purchase to be made in a faster, more secure manner. With offline authorization, data authentication also protects against counterfeit cards.

- The EMV standard also has limits on offline activity, which protects against credit overruns and fraud.

Criteria 3: Respond Appropriately to Suspicious Transactions (so as to limit losses and prevent fraudulent transactions)

- EMV standards provide issuers the ability to define card usage restrictions such as international use prohibitions or limits on the number of transactions conducted in a defined time period.

- Issuer Scripting allow issuers to manage their cards in the field to provide better fraud protection. These scripts can be used to manage offline spending limits defined on the card, or disabling the card from working with EMV terminals.

Criteria 4: Secure Debit Card and Cardholder Data

- With online authorization, cryptographic data is generated based on the terminal's computer, the card's on-board processor, and the transactional data, protecting against the use of skimmed data and stolen account data

CONCLUSION

The SIDC commends the Board for a remarkable job in broaching the issue of financial card fraud prevention through the issuing of this Proceeding. By doing so, it has signaled its consideration of the American consumer's best interests, not only with regard to their economic health, but to their financial privacy and data security.

The SIDC offers its full support to the Board as it works with Congress to determine and develop the proper, explicit legal authority to address the adoption and implementation of a secure financial payment card system in the United States. Further, we encourage the Board to work with privacy professionals and data security experts to create ways to ensure a robust, secure payment system that will protect American consumers both here and abroad, and serve US business interests globally. We look forward to working with the Board to ensure the future of the payment industry, while avoiding solutions that might raise costs to consumers, limit efficiency, or disrupt efforts to provide and manage a global solution to preventing credit and debit card fraud.

Respectfully submitted,

THE SECURE ID COALITION

By:

Kelli Emerick
Executive Director
Secure ID Coalition
919 18th St., NW – Suite 925
Washington, D.C. 20006
Kemerick@SecureIDCoalition.org

ATTACHED: *Myths & Facts About Chip-and-PIN*, Secure ID Coalition

MYTHS & FACTS about Chip-and-PIN

1) **MYTH: New, more expensive cards have to be issued and that will cost the banks extra money.**

   FACT: Banks issue new cards everyday to customers – especially those who experience breaches to their accounts. The cost of that reissuance would cover the cost of the transition to Chip–and-PIN. Not to mention the amount of money saved from the prevention of fraudulent transactions.

2) **MYTH: Merchants will not want to purchase new hardware required for the system.**

   FACT: The point-of-sale (POS) terminals used in most US retail establishments already have a Chip-and-PIN slot, as they are manufactured for a worldwide market. All that is required is a software upgrade to make the slots operational. In the cases where the Chip-and-PIN slot is not currently in the POS terminal – there are two options:

   1) In the case of leased terminals, which most small business use, the leasing agent could provide a new terminal that includes the slot, or
   2) Large stores that purchase their own terminals need to regularly purchase new equipment. POS terminals are typically on a three-to-five year lifecycle and are regularly replaced. In the small instances where terminals have not already been upgraded, the cost of upgraded terminals compared to old swipe terminals is negligible.

3) **MYTH: Consumers will not know how to use the Chip-and-PIN cards and readers and will need to change behavior.**

   FACT: Americans are already acquainted with how Chip-and-PIN technology works. They use a card and enter a PIN millions of times every day at the ATM. Consumers are happy to do anything that is going to protect their personal and financial information. In most retail transactions, a clerk will be present to help those that need assistance.

4) **MYTH: Merchants must already adhere to the Payment Card Industry Data Security Standard (PCI DSS) that requires them to annually validate their compliance or be fined by the issuers (VISA and MasterCard). Why do we need more?**

   FACT: All of the security efforts of the payment system are focused on back-end detection, as opposed to front-end prevention. In recent years PCIDSS has not been an indicator of security, especially considering recent data breaches, such as Heartland Payment Systems in of October 2008. Those standards do nothing to prevent a card number from being used by an unauthorized person for fraudulent purposes. When asked about Heartland, Gartner analyst Avivah Litan, said what's needed is a sweeping overhaul of how payments are handled. "It's a collective problem, it's not just Heartland's problem," she said. "It's Visa's, it's MasterCard's, it's the banks'. … You've got to make some improvements to card technology and cardholder authentication." That is what Chip-and-PIN does for the payment system. Chip-and-PIN will provide the payment industry front end prevention.

5) **MYTH: Networks and processors the process transactions between merchants and banks will need to change their systems and adapt.**

   FACT: Currently, networks and processors are processing transactions for many other countries around the world that are using Chip-and-PIN. Transaction processing of Canadian and Mexican Chip-and-PIN card payments is already happening by these entities without any problem. The suggestion that processors are not already undertaking this transition to Chip-and-PIN is disingenuous.

6) **MYTH: To effectively implement Chip-and-PIN cards from the issuance to the transactions themselves, you're talking about a massive overhaul of the system.**

FACT: Our entire payments system is based on a culture of detection and not prevention. As a result, American consumers are paying for it through fraud and ID theft. Last year identity theft cost Americans $54 billion as reported by Javelin. This only accounts for the fraud we can identify. Clearly the American payments system is broken and needs to be overhauled.

7) **MYTH: The U.S. had already accepted mag-stripe as the industry standard while other countries were still developing their card infrastructure. U.S. card users will not be able to quickly and easily adapt to a new type of payment card.**

FACT: Americans adapt to upgrading technology pretty easily. There were few problems with the transition from VHS tapes to DVDs or the transition from analog to digital television. Upgrading credit card technology to protect personal and financial information is a simple change and less painful than upgrading a cell phone.

8) **MYTH: Telecom in the United States is cheap, ubiquitous and very reliable. As a result, each transaction can be verified online unlike in other nations around the world where the cost of communication is very expensive and it is prohibitive to verify every transaction at point of sale.**

FACT: Even though online verification is easy and cheap in the US, the current payment system is still riddled with fraud, theft and abuse. As a result of superior infrastructure the US market should have the best, most secure and privacy enhancing payments system in the world. Instead, the credit card industry has forced the use of outdated 50-year-old technology that puts personal and financial information at risk and at the same time puts the burden on the consumer to monitor their accounts for fraud that could have been prevented by using Chip-and-PIN.

Chip-and-PIN is an open standard that is used in every G-8 and G-20 country around the world except the U.S. Because the rest of the world is using the more secure Chip-and-PIN, criminals from other countries have flooded the U.S. to take advantage of our unsecure payment system making the US an easy target for fraud, ID theft and criminal activity.

Other technology solutions have been discussed in the media as a possible way to secure the credit and debit card markets and stem the on-coming tide of fraud. Many of those are proprietary technology solutions from companies that have not engaged in any major credit card market. Using such technologies will do nothing to ensure U.S. traveler's credit cards will be secured and accepted at payment terminals in every other country around the world.

It's now up to the industry to begin adopting chip and pin technology currently available and used around the world in order to more securely lock down the sensitive, personal information that is transacted every day. Adopting Chip-and-PIN will allow for more efficient and seamless business, reduce the true cost of fraud in the credit and debit card systems and give consumers stronger faith in the security of the personal information in the financial system.