Secure Remote Payment Council (SRPc)
Routing Competition Regulations
February 27, 2017

Objective

This white paper is the sixth in the series developed by the Secure Remote Payment Council (SRPc). This SRPc position paper provides a deeper dive into the issues regarding lack of Merchant input to debit network routing as a function of EMV implementation. The problem manifested itself at the POS terminal where customers were asked to select debit routing options, without the requisite education on what those options mean. Merchants contend that Merchant choice should dictate how debit routing occurs.

The SRPc reports on the ongoing problem with routing competition regulations and provides an update on the industry response.

Background

In August, the SRPc reported on the problem that arose in the implementation of EMV that deals with customer prompts that appear on the POS screens at the time of checkout. EMV enabled POS terminals were rolled out, prompting consumers to choose a debit route rather than providing merchants with that routing control. Consumers were given a choice of Visa Debit or U.S. Debit, the latter being presented as the option to select for cash back. For MasterCard, the options being presented are MasterCard Debit or U.S. Maestro Debit. Little explanation was provided to the consumer to understand the differences in the options presented.

The options made available in the initial implementation of EMV depended upon what the card issuer has labeled and prioritized on the card for debit and credit - either through the debit networks or the global brands. Issuers are required by the global brand to prioritize their brands and thus the default setting on the terminal did exactly that, eliminating Merchant choice in the process. Many terminals came preprogrammed with the default equipment and software settings on the POS terminal made the customer select either "Visa Debit" or "U.S. Debit."

The issue was further complicated as Merchants were told, depending on how their terminals were configured for EMV, that opting to alter or remove confusing screens would trigger a lengthy and expensive re-certification process, exposing Merchants to chargeback fraud losses after the liability shift date.

Merchants are demanding that their vendors relabel the routing options presented on the card and reconfigure their terminals to preserve their Durbin Amendment Regulation II debit routing rights.

It is important to note that some Merchants configured the terminal prompts to work the same way that they did pre-EMV implementation for magnetic stripe using cancel or credit/debit function buttons. These Merchants did not experience these debit routing problems. Based on a recent clarification from the Federal Reserve on Regulation II merchant routing rights, Merchants can perform whatever cardholder verification method they prefer and route to their preferred network provider. Some global card networks contend that Merchants should also allow the customer to initiate a transaction with a global brand using either PIN or signature.

Government Agency Response

The issue of Merchant routing choice continued to be a contentious one causing the Federal Reserve and the Federal Trade Commission to weigh in on the subject of debit network routing.

The Federal Trade Commission (FTC) began investigating Visa Inc.'s practices involving EMV debit card transaction routing. The probe started July 2016 when the FTC conducted an investigation into Visa's requirements for EMV debit routing practices, expressing concerns about potential violations to Regulation II of the Dodd Frank Amendment on PIN Debit gateway routing.

Then on November 2, 2016, the Federal Reserve issued objections to Visa's practices on EMV routing from Merchant terminals, based on the customer selection. The objections surfaced in the form of Q&A responses to an online notice posted on the Fed's web site on Regulation II. In their response, the Fed affirmed that no one can inhibit the ability for the Merchant to make the routing choice, and any EMV chip application that routes only to a single network is in violation if that application is isolated based on any selection prompts at the point-of-sale.

In that same timeframe, eight Merchant Associations sent a letter to Visa about what they view as violations to the 2010 Dodd Frank Act's Durbin Amendment relating to debit routing. Merchants demanded the choice of two unaffiliated networks for EMV debit routing, and stated that other stakeholders cannot interfere with Merchant choice for routing. The Merchant Associations include Retail Industry Leaders Association (RILA), the Merchant Advisory Group, National Association of College Stores, NACS (the National Association of Convenience Stores), National Grocers Association, National Retail Federation, Petroleum Marketers Association of America, and the Food Marketing Institute.

Merchants contend that Visa presented confusing POS screen prompts to consumers when Visa cards were inserted. Some large merchants have accused MasterCard of the same. Furthermore, the Merchants contend that the Fed's response was the result of purposeful steps by Visa to circumvent network routing choice by Merchants, and they demanded the Fed address and remediate these violating practices.

Response from the Global Brands

Visa made a clarifying announcement in June stating that Merchants can use whatever card verification method (e.g., PIN, signature, or no CVM), but in every case the transaction must be able to be routed to Visa. The Merchants were still not satisfied that they controlled debit routing, as evidenced by the decline in U.S. debit network transaction volumes compared to pre-implementation levels.

This November, in response to industry backlash, Visa amended their EMV documentation on Merchant choice for routing debit transactions, stating that all debit transactions can be routed using the U.S. Common Debit AID, notwithstanding the customer's choice of card verification method, adding that cardholders are not prompted to select the AID (i.e., Visa Debit or US Debit) for routing. Appendix F of the Visa Transaction Acceptance Device Guide was also amended, stating that the U.S. covered Visa debit cards are issued with both the Visa AID and the U.S. Common Debit AID.

On the use of U.S. EMV enabled debit cards, Visa provided further clarification on the subject, stating:

- Merchants have flexibility to use either the U.S. Common Debit AID or the Visa AID. Merchants are never required to use the Visa AID to process U.S. debit transactions, and they can route exclusively to the U.S. Common Debit AID if they choose regardless of the card verification method or the network they are routing to, including VISA or MasterCard.
- Merchants are never required to ask the cardholder to choose the AID for processing debit transactions.
- Merchants can promote their preferred card verification method. They can prompt for a PIN, and even discourage the use of signature but must provide the cardholder with the option to perform the transaction using signature or "No CVM."
- When the cardholder selects the U.S. Common Debit AID, BIN routing logic will transmit the transaction to the designated debit network including VISA or MasterCard. When the cardholder selects the Visa AID, the transaction must be routed to Visa.

The SRPc notes that even with the aforementioned rule changes, Visa is not making the Common Debit CVM card verification method available to the other U.S. debit networks. Furthermore, that global card brands must license out all CVMs, including biometrics and other emerging technologies to the Common AID on the EMV application ID for issuers and global networks to be in compliance with Regulation II as clarified by the Federal Reserve.

In addition, there are a growing number of purchase transactions not performed at the physical point-of-sale that do not use EMV, but utilize tokens that cannot be routed to networks other than VISA or MasterCard for authorization. These tokens cannot be processed by other debit networks. By not allowing debit networks the ability to process these purchases it is difficult for issuers to abide by Regulation II routing rules.

SRPc Call to Action

In light of the events which occurred as a result of EMV implementation, the SRPc has been compelled to reiterate its industry “Call to Action” reaffirming its position on fair and equitable treatment for all industry stakeholders where payment routing and security are concerned.

- *Enforce Change* - The Federal Trade Commission has conducted the investigation and determined that Merchant choice for debit routing must be upheld. Now that the decision has been made, it is incumbent upon the FTC to enforce this change in accordance with the Fed’s commentary.
- *Liability Relief* – Changes to the POS terminal and the resultant certification and testing takes time to execute. Merchants have ongoing concerns about chargeback liability exposure as these changes are placed into effect. The SRPc endorses a change in policy that provides Merchants with both liability and financial relief as changes to the offending POS screens are made.
- *Clarified Application to Non-Face-to-Face Transactions* – As Merchants expand their payment processing capability to the online and mobile platforms, the same considerations must be made for debit routing. It may be the case that domestic debit networks around the world have more power than the U.S. debit networks have had to get these types of regulations recognized by the global brands. The SRPc calls upon the industry to make certain that policy makers support the same routing provisions in the online and mobile channels as those in the tradition POS in order to ensure debit routing provisions, as clarified by the U.S. Federal Reserve, are in compliance with Regulation II. The Federal Reserve’s FAQs make very clear that these routing provisions can and should apply to mobile and ecommerce.
- *New Terminology* – The SRPc contends that part of the problem with the debit routing choice is that the terminology U.S. Common Debit AID is vague and non-descriptive, and as such, recommends changing the language to something more recognizable and clear to the consumer.
- *Increased Safety and Security* - In its current implementation, the EMV chip technology is underutilized, as chip and signature was implemented instead of chip and PIN. The SRPc strongly endorses the implementation of chip and PIN, and advocates for using the computational power of the chip to protect the PAN for added safety and security. Interoperability is the key.
- *Cross Border and Global Expansion* – The discussion on Merchant debit routing has focused on issues relating to the implementation in the U.S. market. Longer term, the payments industry will need to expand its EMV reach to include cross border and global transactions. While the U.S. domestic debit network requirements are somewhat unique to the U.S., these same Merchant debit routing requirements must be supported on a global basis.
- *Open Standards & Inclusive Technology* - Current EMVCo standards are proprietary and as such, U.S. domestic debit networks were segregated to the Common Debit AID which licensed the EMV Chip Application ID with usage under restrictive terms. In the future, Merchants want the EMVCo brands to open up the Global AID on the EMV Chip Application to all U.S. domestic debit networks. The SRPc contends that an industry standard for payment must be developed in an open forum where all industry stakeholders have a voice in the outcome.

About the Secure Remote Payment Council

The Secure Remote Payment (SRPc) is a nonprofit, inter-industry trade association that supports the growth, development and market adoption of debit based internet eCommerce and mobile channel payment methods that meet or exceed the security standards for pinned based card present payments. It will accomplish this by encouraging and supporting those activities that accelerate the implementation, adoption and promotion of these payments. The SRPc’s members include merchants, financial institutions, merchant processors, issuer processors, payment brand companies, payments authentication hardware providers, payments authentication software providers and payments consultants. This document does not necessarily express the views and opinions of every member of the SRPc. For additional information, visit SecureRemotePaymentCouncil.