



**Secure Remote Payment Council (SRPC)  
Federal Reserve Payment Study - Request for Comment  
Depository and Financial Institution Payments Survey (FR 3066a)  
December 19, 2012**

On behalf of the Secure Remote Payments Council (SRPC), we appreciate the opportunity to contribute the following commentary on The 2013 Federal Reserve Payment Study on Depository and Financial Institution Payments.

Specifically, the SRPC comments address Section 10 in the survey collection instrument which deals with third-party payment fraud.

Section 10: *Third-Party Payment Fraud* - Respondents would report the number and value of unauthorized check payments, unauthorized ACH credits and debits, unauthorized debit and prepaid card transactions, unauthorized credit card transactions, and unauthorized ATM cash withdrawals. The Board specifically requests comment on whether institutions can report information on unauthorized transactions, as defined, or whether another definition of third-party fraud would be more feasible and/or useful to report.

The SRPC agrees that Section 10 should be added to the survey because it is important to capture data about the volume and value of unauthorized transactions in noncash payment systems as a way to estimate, with some level of consistency, the fraud rate for those payment options.

The SRPC comments address the definition of “Unauthorized Debit Transactions” as described in the survey collection instrument. Perhaps the important aspect of this survey is to make sure there is a common understanding for the definition of fraud. “Authorized” is intended to mean any transaction that was authorized by the Issuer or its designated processor. It does **not** include transactions that the merchant authorized, transactions that were completed without an authorization, or fraudulent transactions committed by the cardholder “friendly fraud.”

Fraud should be broken down into its most granular level so that it can provide useful information for different stakeholders. This table may help visualize how the SRPC is recommending fraud should be reported. Fraud should be first segmented by authentication type, and then further delineated by acceptance channel. (Note that this table also includes a construct for collecting information on “Authorized Debit Transactions” as requested in Section 6. Debit and Prepaid Cards.)

	Section 10. Origin of Debit and Prepaid Card Fraud Losses											
	By Authentication Type											
	10.A PIN				10.B Signature				10.C No Signature / Unattended Device			
	Transaction Count		\$ Amount		Transaction Count		\$ Amount		Transaction Count		\$ Amount	
	Auth	Non-Auth	Auth	Non-Auth	Auth	Non-Auth	Auth	Non-Auth	Auth	Non-Auth	Auth	Non-Auth
<b>By Acceptance Channel</b>												
1. Card-Present (CP) Magnetic Stripe		A1		A1		B1		B1		C1		C1
2. Card-Present (CP) CHIP		A2		A2		B2		B2		C2		C2
3. Card-Not-Present (CNP)		A3		A3		B3		B3		C3		C3
<b>Total Fraud</b>												

Areas shaded in green are relevant to Section 10: Third-Party Payment Fraud, and the numbering scheme corresponds with the definitions below.

The SRPc suggests that unauthorized transactions should be segmented into three distinct categories by method of authentication, namely:

- Unauthorized PIN Debit transactions
- Unauthorized Signature Debit transactions
- Unauthorized No-Signature Debit transactions

The category “No-Signature” is designed to capture debit transactions performed at an unattended device. All such devices have a specific merchant classification code (MCC) and Issuers track fraud data by MCC code. For example, the most common automated device is Automated Fuel Dispensers (AFD). AFDs are designated MCC code 5542.

The definitions of these authentication categories are provided as follows:

**10.4 Unauthorized debit and prepaid card transactions = March - Number and Value \$**

**Include:** All unauthorized debit and prepaid card transactions, before any recoveries or chargebacks, for which your institution was the card issuer. All fraudulent transactions made either by debit cards linked to a deposit account or prepaid cards for which your institution was the card issuer. Include only transactions that were not authorized by a legitimate cardholder (third-party fraud).

**Do not include:** Debit and prepaid card fraud prevented before a loss was incurred, fraud committed by a legitimate cardholder (first-party fraud), fraudulent credit card transactions, fraudulent ATM withdrawals, or debit and prepaid card transactions authorized by a legitimate cardholder as part of a scam.

**10.4A. Unauthorized PIN transactions = March - Number and Value \$**

**Include:** Unauthorized transactions over a PIN (single-message) debit card network, before any recoveries or chargebacks, for which your institution was the issuer. Fraudulent PIN transactions made either by debit cards linked to a transaction deposit account or prepaid cards for which your institution was the card issuer.

**Do not include:** Unauthorized signature or no-signature transactions.

**Note:** This is a subset of item 10.4 above.

**10.4B Unauthorized signature transactions = March - Number and Value \$**

**Include:** Fraudulent transactions over a signature (dual-message) debit card network, before any recoveries or chargebacks, for which your institution is the card issuer. Fraudulent signature transactions made either by debit cards linked to a deposit account or prepaid cards for which your institution was the card issuer.

**Do not include:** Fraudulent PIN transactions, or unauthorized signature transactions where no physical signature is provided from the cardholder.

**Note:** This is a subset of item 10.4 above.

**10.4C Unauthorized no-signature transactions = March - Number and Value \$**

**Include:** Fraudulent transactions over a signature (dual-message) debit card network *where no physical signature from the cardholder is provided*, before any recoveries or chargebacks, for which your institution is the card issuer. Fraudulent no signature transactions made either by debit cards linked to a deposit account or prepaid cards for which your institution was the card issuer.

**Do not include:** Fraudulent PIN transactions, or unauthorized signature transactions performed where a cardholder signature was obtained.

**Note:** This is a subset of item 10.4 above.

The SRPc also recommends that the definitions in Section 10.4 make a clear distinction about transactions performed at the acceptance channel, namely card-present (CP) vs. card-not-present (CNP).

The definitions should also address the form factor being used. For example, the definitions segment Signature and PIN but should further differentiate between Magnetic Stripe and Chip. This will enable a further distinction for Issuers that are issuing Chip & PIN even to those transactions routing signature-debit (dual-message).

The definitions of these acceptance channels are provided as follows:

**4.1. Card-present transactions: Magnetic stripe March - Number and Value \$**

**Include:** Unauthorized debit transactions performed with a magnetic stripe card, before any recoveries or chargebacks, for which your institution was the card issuer and the card was present at the point of sale.

**Do not include:** Unauthorized Internet, mail order, or telephone transactions.

**4.2. Card-present transactions: Chip March - Number and Value \$**

**Include:** Unauthorized debit transactions performed with a contactless or contact chip card, before any recoveries or chargebacks, for which your institution was the card issuer and the card was present at the point of sale.

**Do not include:** Unauthorized Internet, mail order, or telephone transactions.

**4.3. Card-not-present transactions: March - Number and Value \$**

**Include:** Unauthorized debit transactions, before any recoveries or chargebacks, for which your institution was the card issuer and the card was not present at the point of sale, such as an internet, mail order, or telephone transaction.

**Do not include:** Unauthorized card-present transactions.

The SRPc suggests that output from the card issuers completing this survey will be significantly enhanced if the data requested was structured in accordance with the transactions codes supported by Visa and MasterCard, and thus we are recommending that construct for data collection. At minimum, the Issuers should be able to break down their categories of fraud by authentication type (PIN vs. Signature) and acceptance channel (CP vs. CNP). Any further refinement will provide greater insights into the categorization of fraud.

Furthermore, the SRPc acknowledges that there are many different ways to report fraud, but the data that would be most valuable to the industry would be that which reports hard (i.e., uncollectible) losses due to fraud. As such, Issuers completing this survey should be instructed to purposefully exclude those chargeback losses for transactions that were authorized, but the Issuer nonetheless was required to pay.

One final comment: There may be some benefit to separating debit and prepaid transactions, creating each as its own major payment category in both Sections 6 and 10 of the survey. Bank Issuers do have to complete Quarterly Assessments for Visa and MasterCard to report fraud losses, and it is our understanding that Issuers must report prepaid separate from signature debit. This should make it easy for the Issuers to extract this information for this survey data collection.

Although a prepaid transaction is processed as a signature debit transaction, the distinction between these payment types is particularly important in the case of tracking third-party fraud. While the fraud losses associated with a general purpose reloadable (GPR) prepaid transaction and a signature debit transaction are comparable, the frontload on a general purpose reloadable card is a very high risk transaction – one that is unique to prepaid cards. This risk is particularly high for government-issued GPR cards, e.g., those issued for tax refunds. Some Issuers will not support frontloads using a signature debit card; they will only allow frontloads to be performed with a credit card. In light of this, the SRPc suggests that a separate fraud category should be created to address prepaid frontload fraud, either as a specific line item in the credit card fraud section, or under prepaid card fraud section, separate from debit.