Chargeback Best Practices

September 7, 2016

U.S. Payments Forum

… the cross-industry body focused on supporting the **introduction and implementation of EMV and other new and emerging technologies** that protect the security of, and enhance opportunities for payment transactions within the U.S.

- Established in 2012 as the EMV Migration Forum, which has been instrumental in the progress of the U.S. migration to EMV chip technology
- Full payments ecosystem membership
  - Issuers, merchants, acquirers/processors, payment networks, consultants, integrators, industry suppliers, industry associations

US PAYMENTS FORUM

EMV in the U.S.

- Significant progress has been made with EMV migration
  - Over 500 million EMV chip cards have been issued
  - Over 1.7 million merchant locations are accepting chip transactions[1]
  - 11.1% of Visa transactions are chip-on-chip[2]
- **Goal of EMV**: Prevent card-present fraud at the retail POS
  - 38% decrease in counterfeit fraud at merchants accepting chip[2]

[1] Digital Transactions, Aug. 12, 2016 , http://www.digitaltransactions.net/news/story/6336
[2] Digital Transactions, Aug. 24, 2016, http://www.digitaltransactions.net/news/story/Visa-Says-Chip-on-Chip-Transactions_-a-Key-Metric_-Have-Grown-26_-Since-May

US PAYMENTS FORUM

Fraud Liability Shifts and Chargebacks

- **Fraud Liability Shifts**
  - Shift the responsibility for any fraud resulting from a payment transaction to the party using the least secure technology
  - **Driver** -- reduce fraud by encouraging EMV migration by both issuers and merchants
- **Chip Liability Shift (CLS) Chargebacks**
  - Result from the U.S. not being 100 percent chip-enabled
  - New policies related to frequency and minimum value
  - **Webinar focus** -- present best practices for issuers, merchants and acquirers to:
    - Ensure valid authorizations and avoid CLS chargebacks
    - Manage disputes and mitigate chargebacks

US PAYMENTS FORUM

Webinar Agenda

- **Introduction and Market Status**
  - Randy Vanderhoof, U.S. Payments Forum
- **Issuer Authorization Best Practices**
  - Simon Hurry, Visa Inc.
- **Merchant Best Practices for Authorization and Avoiding Chargebacks**
  - Steven Cole, Vantiv
- **Issuer Best Practices for Managing Disputes**
  - Brandon Cranford, Woodforest National Bank
- **Merchant Best practices for Disputing and Mitigating Chargebacks**
  - Doug Whiteside, MasterCard
- **Conclusions and Q&A**
  - Randy Vanderhoof, U.S. Payments Forum

US PAYMENTS FORUM

Issuer Authorization Best Practices

Simon Hurry, Visa Inc.

General Principles

Three basic principles should guide issuer authorizations

- Maintain or strengthen risk controls on magnetic stripe transactions
- Relax risk controls on chip on chip transactions
- Strengthen risk controls on fallback transactions

US PAYMENTS FORUM

Additional Issuer Best Practices

Data Quality and Common Sense Checks

- Check that the POS Entry mode matches the product capabilities for the payment device issued
- Check and validate the service code and CVV and decline invalid CVV codes on magnetic stripe swipes
- Use industry risk scoring tools to manage fraud risk
- Use a robust risk rules engine to manage fallback
- Perform velocity checks for uncommon usage patterns
- Use travel alerts or location checks as additional safeguards

US PAYMENTS FORUM

Issuer Guidance to Cardholders

Cardholders can play an important role in preventing fraud

- Encourage cardholders to set up alerts
- Encourage cardholders to advise issuers on dates of overseas travel
- Encourage cardholders to monitor their accounts frequently, preferably online, but also by calling the number on the back of the card
- Encourage cardholders to report a lost or stolen card or mobile phone with a mobile payment app immediately to the issuer

US PAYMENTS FORUM

US PAYMENTS FORUM

Merchant Best Practices for Authorizations and Avoiding Chargebacks

Steve Cole, VANTIV

Merchants Not Yet Chip Enabled

- May face increasing threat of counterfeit transactions from card fraud rings
- Fraudulent mag-stripe transactions may result in increased CFLS chargeback liability
- Until chip-enabled, there are some best practices that can help reduce fraud for POS transactions

US PAYMENTS FORUM

Merchants Not Yet Chip Enabled

- Read and Compare Verification
  - Verify last 4 digits of number on card against number read off mag-stripe
  - Especially relevant when:
    - Transactions over a specific dollar amount
    - Purchases of items associated with high fraud
    - Transaction is suspicious

US PAYMENTS FORUM

Merchants Not Yet Chip Enabled

- Check Cardholder's ID, If Necessary
  - Check name on card matches name on ID
  - Some networks do not allow ID checks as a condition of the sale and doing so may have non-compliance implications
- Perform Velocity Checks
  - Highlights excessive transaction activity
  - May not be fraud, but could be used to trigger additional verification steps

US PAYMENTS FORUM

Merchants Not Yet Chip Enabled

- Establish Strategy for Transactions That May Involve Counterfeit
  - Identify targeted goods, services or locations
  - Implement procedures to address fraud targets
    - Have manager or specific terminal to process gift card purchases above a specific dollar amount
    - Contact issuers to approve specific high risk transactions and/or to confirm cardholders
- Implement PIN Prompting for Debit Transactions
  - Capturing a knowledge-based verification method at the POS can reduce fraud

US PAYMENTS FORUM

Merchants That Are Chip Enabled

- Fallback
  - Could indicate a fraudster has tampered with the chip or the magnetic stripe is counterfeit
  - Terminal must accurately identify its capabilities
- PIN Support
  - For networks with LSLS, merchants are encouraged to certify online and offline PIN for debit and credit

US PAYMENTS FORUM

Merchants That Are Chip Enabled

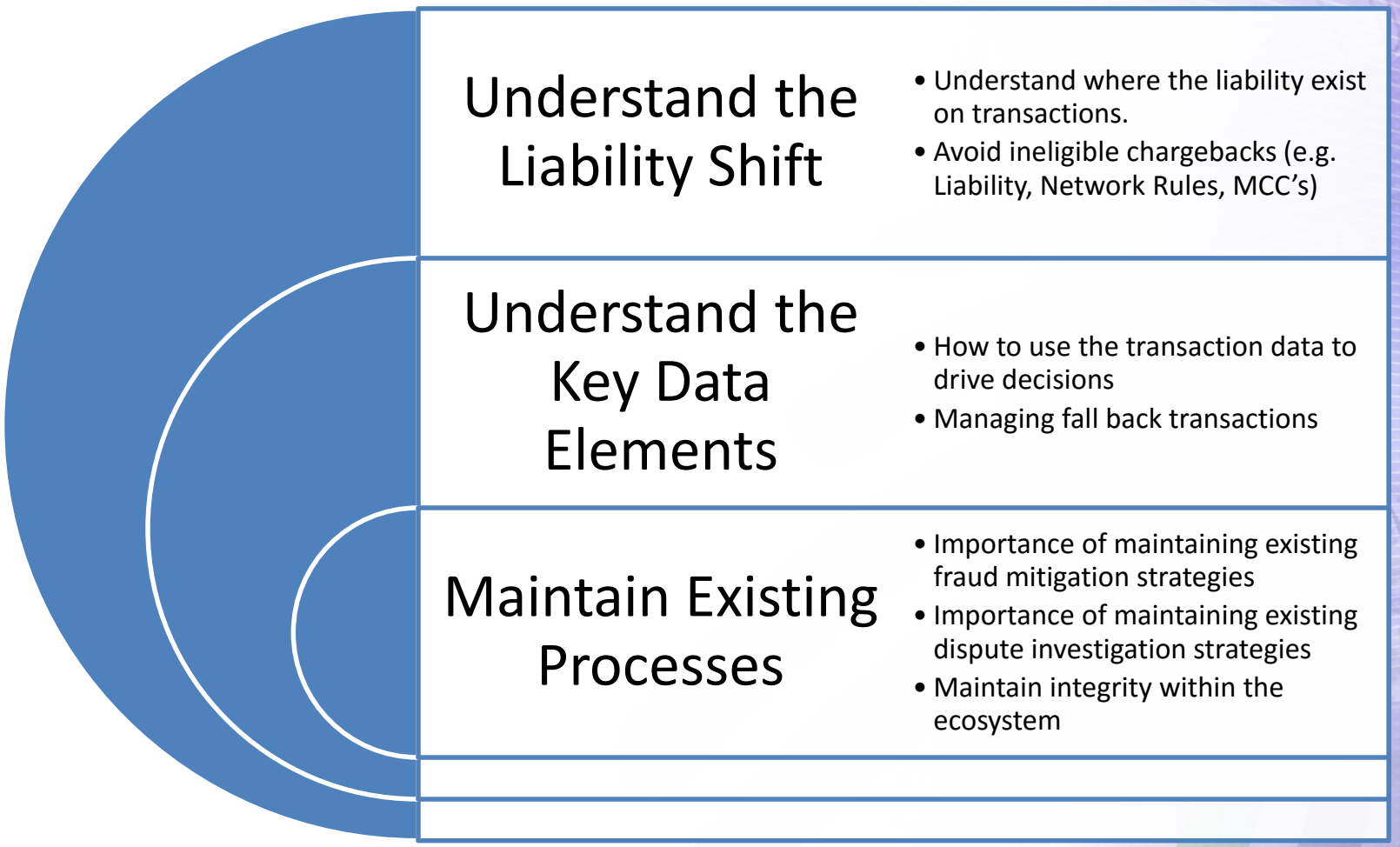
- Data Quality
  - Critical to maintain data integrity/accuracy across authorization and settlement messages
  - Differing TEC values may result in erroneous chargeback reason codes by the issuer

US PAYMENTS FORUM

Issuer Best Practices for Managing Disputes

Brandon Cranford, Woodforest National Bank

Issuer Best Practices for Chargebacks



US PAYMENTS FORUM

Merchant Best Practices for Disputing and Managing Chargebacks

Doug Whiteside, MasterCard

Guidance on Merchant Best Practices

- Many merchants have deployed chip terminals in stages, with chip terminals in one location while continuing to operate magnetic stripe terminals in another. In any dispute, the authorization information (not the clearing information) for each individual transaction will help determine the validity of the reported CLS chargeback.
- When a CLS chargeback is valid, it is essential that the acquirer not re-present the chargeback. Like invalid chargebacks, invalid re-presentments are costly to both the acquirer and issuer.

US PAYMENTS FORUM

Guidance on Merchant Best Practices

Key Data Points – The minimum data merchants and acquirers should maintain include:

Counterfeit	POS Entry Mode; Service Code; Issuer Approval Code; Terminal Entry Capability; Attended Terminal Status and evidence that the Chip Data/Field 55 was sent
Lost or Stolen	POS Entry Mode; Service Code; Issuer Approval Code; Terminal Entry Capability; Attended Terminal Status; Evidence that Chip Data/Field 55 was sent; Terminal PIN Pad Status in Chip Data/field 55; Terminal Verification Results (TVR); Card Verification Results (CVR) and the POS PIN Entry Mode

The relevant data varies by payment network and where the data may reside in the message may vary by payment network. Contact the acquirer for more information on network-specific message formats and data.

US PAYMENTS FORUM

Guidance on Merchant Best Practices

Valid reasons an acquirer or merchant may re-present a CLS chargeback, including but not limited to the following:

- Invalid documentation - The cardholder fails to state the card is in their possession (counterfeit CLS) or the card was lost/stolen (chip/PIN CLS) and not in their possession *(if the network requires the information to be provided to the acquirer)*
- The transaction was not properly reported as fraud according to the brand or network CLS chargeback requirements
- The service code appearing in the authorization is not 2XX or 6XX *(card accepted at POI as a magnetic stripe card)*

US PAYMENTS FORUM

Guidance on Merchant Best Practices

Continued:

- The transaction was identified as an AFD in the authorization *(this chargeback is invalid until October 2017)*
- The transaction was identified as a contactless transaction
- Authorization data confirms the card and the terminal were EMV enabled and valid data supports proper processing
- Lost/Stolen - Authorization data confirms that the EMV terminal supports online and offline PIN and the terminal PIN pad was operating properly at the time of the transaction

US PAYMENTS FORUM

Conclusions

Randy Vanderhoof, U.S. Payments Forum

Conclusions

- Many chargebacks result from fraud that was already in the system but was not visible to many stakeholders as issuers historically absorbed this fraud in the face-to-face environment
- Avoiding chargebacks hinges on the transaction authorization process and data integrity
- Chargebacks and card-present disputes are expected to decrease as:
  - Chip implementations become more robust and data quality improves
  - Fraud is reduced by EMV implementation

US PAYMENTS FORUM

Q&A

US PAYMENTS FORUM

www.uspaymentsforum.org

U.S. Payments Forum Resources

- EMV resources: www.emv-connection.com
  - EMV Chargeback Best Practices white paper
  - Minimum EMV Chip Card and Terminal Requirements
  - Understanding the 2015 U.S. Fraud Liability Shifts
  - Many other white papers, webinars and video recordings on EMV implementation topics
- U.S. Payments Forum information: www.uspaymentsforum.org

- **Randy Vanderhoof**, rvanderhoof@uspaymentsforum.org
- **Simon Hurry**, shurry@visa.com
- **Steven Cole**, steven.cole@vantiv.com
- **Brandon Cranford**, bcranford@woodforest.com
- **Doug Whiteside**, doug.whiteside@mastercard.com

US PAYMENTS FORUM

www.uspaymentsforum.org