EMV Chargeback Best Practices

Version 1.1

Date: April 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

The U.S. Payments Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The U.S. Payments Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: transaction-speed@uspaymentsforum.org.

Table of Contents

1. Introduction

Fraud impacts all stakeholders. When counterfeit or lost and stolen fraud does occur, a cardholder may lose trust in their card product, in their bank and in the merchant where the fraud occurred; the issuer will typically close the account and may risk losing the cardholder when doing so; and a merchant will lose revenue associated with the fraudulent purchase. EMV is being implemented in the United States, as it has in other countries, with the goal of reducing card-present fraud. In particular, counterfeit card-present fraud represents a significant percentage of the overall payment card fraud in the U.S.[1] and EMV has been shown to be an effective tool in reducing this fraud[2,3] once the number of chip-enabled cards and chip-supporting payment acceptance devices reaches a critical mass.

Changes in payment network rules that took effect starting in October 2015 seek to support the migration to EMV by placing liability for fraud – counterfeit, and in the case of most networks, also lost and stolen – with the party to the transaction that has not successfully transitioned to EMV chip technology.[4] In connection with the migration to EMV in the U.S. and the implementation of payment network counterfeit and lost/stolen fraud liability shifts, chargeback reason codes were established for (1) counterfeit, and (2) lost/stolen EMV chip card transactions covered by those chip liability shifts (CLS) ("CLS chargebacks"). Within the overall liability shift, this white paper refers to both counterfeit liability shift chargebacks ("CFLS chargebacks") and lost/stolen liability shift chargebacks ("LSLS chargebacks").

These new chargeback reason codes are a result of the fact that the U.S. is not 100 percent chip enabled in terms of cards and acceptance terminals. CLS chargebacks are expected to gradually decrease as merchants and issuers successfully migrate closer to 100 percent use of EMV technology. It is important to recognize that, for the most part, these chargebacks are resulting from fraud that was already in the system but not visible to many stakeholders as issuers historically absorbed this fraud in the face-to-face environment. Liability shifts have been implemented in all countries that migrated to EMV; thus the CLS aligns the U.S. market with all other chip markets. However, with these new types of chargebacks, U.S. issuers, acquirers and merchants alike are appropriately concerned that they fully understand the chargebacks and that all such new chargebacks are validly issued.

In order to help ensure that purported CLS chargebacks are valid, there are network requirements that issuers must meet and networks should monitor chargeback activity for validity. There are a number of other steps that issuers, acquirers and merchants can take, including steps to help ensure the quality of the data and the integrity of related processes. Taking these steps will in turn help to minimize the number of chargebacks opened.

This paper is specifically focused on the appropriate treatment and mitigation of these new CLS chargeback types for contact chip cards used in attended transactions only and only for those chargebacks occurring after the liability shift dates. Out of scope for this paper is discussion of other chargeback types, including but not limited to those for unattended transactions and the transactions described in Section 4.1.2 below.

[1] "Global Card Fraud Damages Reach $16B," PYMNTS.com, August 6, 2015, http://www.pymnts.com/news/2015/global-card-fraud-damages-reach-16b/

[2] "Card fraud figures," UK Cards Association, http://www.theukcardsassociation.org.uk/plastic_fraud_figures/

[3] "Credit Card Fraud and Interac Debit Card Statistics – Canadian Issued Cards," Canadian Bankers Association, July 2015, http://www.cba.ca/contents/files/statistics/stat_creditcardfraud_en.pdf

[4] See "Understanding the 2015 U.S. Fraud Liability Shifts," Version 1.0, U.S. Payments Forum white paper, May 2015, http://www.emv-connection.com/understanding-the-2015-u-s-fraud-liability-shifts/.

2. Issuer Best Practices for Authorization

The primary goal of issuers is to reduce or eliminate fraud wherever possible without compromising the user experience for the valid cardholder with a valid card. Regardless of whether an issuer's portfolio is chip enabled or not, it is very important to the prevention of fraud, that an issuer maintains its risk management controls and aims to ensure a true risk-based authorization response.

Following a claim of fraud from a cardholder, the issuance of a valid chargeback by an issuer rests primarily on the authorization response to a transaction. There are several best practices that issuers may follow to ensure the integrity of authorization responses.

2.1 Issuer Authorization Best Practices

2.1.1 Magnetic Stripe Cards at any Terminal

If an issuer has not yet issued chip cards, or has begun but has not completely replaced all magnetic stripe cards with chip cards, they are strongly encouraged to continue to follow the risk management protocols in place today, as well as use the risk management tools available to them to detect and decide whether to decline high risk transactions.

In addition, issuers are encouraged to check and validate the service code sent in the transaction data from the card, and the transaction type, because these data elements indicate whether the origin of the data was a chip card and whether the card was swiped or inserted. It is important for issuers to compare the data they are seeing in the transaction record to their expectation regarding that account's cards. In general, issuers should only be authorizing transactions that match the product capabilities for that account. For example, if an issuer has implemented neither chip nor mobile wallet technology, they should decline transactions with indicators showing that transactions originate from chip or mobile device. In addition, an alteration of the first digit of the service code may indicate an attempt at fraud and should be declined.

As with all magnetic stripe transactions the card security code[5] on the magnetic stripe should be checked and validated, since the card security code prevents fraudsters from altering values such as the expiration date on the card.

Lastly, issuers should implement velocity checking, and/or look for transactions that do not seem appropriate or normal from the perspective of the purchase history of the cardholder.

2.1.2 Chip Cards at a Magnetic Stripe Terminal

If an issuer has issued chip cards, those cards will still be used at merchants who have not yet migrated to chip. As in the previous section, issuers are strongly encouraged to continue to follow the risk management protocols in place for magnetic stripe cards, as well as use the risk management tools available to them to detect and decide whether to decline high risk transactions.

Once again, issuers should check and validate the service code on the chip card and the transaction type. In this case, however, they should decline chip card transactions with any service code starting with a number other than 2 or 6. The number 1 or 5 (or any value other than 2 or 6) in the first digit of the service code may indicate an attempt by a fraudster to alter the service code; the issuer should therefore validate the card security code and decline the transaction if the validation fails.

[5] Card security code examples: CSC, CID, CVC or CVC2, CVV or CVV2, PCSC

As with all magnetic stripe transactions the card security code on the magnetic stripe should be checked and validated, since the card security code prevents fraudsters from altering values such as the expiration date on the card.

Lastly, issuers should implement velocity checking, and/or look for transactions that do not seem appropriate or normal from the perspective of the purchase history of the cardholder.

2.1.3 Chip Cards at a Chip Terminal

If an issuer has issued chip cards, and the card is used at a successfully certified EMV-capable terminal, issuers may wish to consider adjusting their risk protocols, since there is a high degree of certainty that the transaction is genuine if processed as a chip-on-chip transaction.

With an online-authorized chip-on-chip transaction, issuers should check and validate the online cryptogram on both contact and contactless transactions. In these transactions, Application Transaction Counter (ATC) tracking, the results of offline data authentication, the service code and CVV checks are largely irrelevant, as the security is based on the validation of the online cryptogram.

However, issuers should still implement velocity checking, or look for transactions that do not seem appropriate or normal from the perspective of the purchase history of the cardholder. This is to prevent and mitigate account takeover and lost and stolen fraud, assuming the cardholder has not reported that their card was stolen.

In the event of a fallback transaction,[6] issuers may want to verify data integrity by confirming the terminal capability is properly indicated by the merchant when fallback is performed, as fallback transactions should never occur on terminals that are not chip capable.

2.2 Issuer Guidance to Cardholders

Preventing fraud is everyone's business and there is a lot that cardholders can do to help and protect themselves against the inconvenience of fraudulent transactions. The following is a list of best practices and guidance issuers can provide to cardholders.

- Encourage cardholders to set up alerts.
- Encourage cardholders to advise issuers on dates of overseas travel.
- Encourage cardholders to set up travel alerts when traveling.
- 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.

[6] A fallback transaction occurs when a transaction is initiated between a chip card and a chip terminal but chip technology is not used and the transaction is completed via magnetic stripe or key entry.

3. Merchant Best Practices for Obtaining an Authorization Response and Avoiding CLS Chargebacks

3.1 Merchants Who Are Not Yet Chip-Enabled

Merchants who have not fully implemented EMV chip acceptance technology (or who have decided to retain magnetic stripe terminals alongside their EMV acceptance devices) may face an increasing threat of counterfeit transactions as card fraud rings focus on targets where magnetic stripes are readily accepted. Furthermore, depending on applicable network liability shift rules and policies,[7] these fraudulent magnetic stripe transactions may result in increased CFLS chargeback liability on transactions where the counterfeit card data originated from a chip card.

While the best defense against counterfeit fraud is to implement EMV chip technology, there are some best practices that merchants can implement to help reduce fraud for point-of-sale (POS) transactions before migrating to EMV.

3.1.1 Read and Compare Validation

Read and compare verification is a process under which the cashier enters the last four digits of the card number embossed (or printed) on the card, and the terminal validates these numbers against what was physically read off the magnetic stripe. If these digits do not match, then there is a high degree of certainty that the card is counterfeit and merchants may wish to cancel the transaction and request another form of payment. Read and compare can also be manually performed by comparing the last four digits printed on the card with the last four digits on the receipt.

Read and compare verification is especially relevant when:

- Transactions over a specific dollar amount are processed
- Purchases involve items known to be associated with high fraud
- The transaction is suspicious

3.1.2 Check Cardholder's ID, If Necessary

If a transaction is suspicious, cashiers may ask the cardholder for an additional form of identification to check if the name on the card matches the form of identification to reduce the possibility of fraud. If additional identification cannot be provided or is provided but does not match the name on the card, merchants can consider the transaction high risk, adhere to merchant store procedures, and respond accordingly.

Merchants are advised to check with their acquirers for information on payment network requirements for checking cardholder identification. For many networks, merchants are not allowed under their network rules to make the identification check process a condition of the sale. Declining transactions due to a cardholder failing the merchant's cardholder identification check may have other non-compliance penalties.

[7] "Understanding the 2015 U.S. Fraud Liability Shifts", Version 1.0, U.S. Payments Forum white paper, May 2015http://www.emv-connection.com/understanding-the-2015-u-s-fraud-liability-shifts/.

3.1.3 Perform Velocity Checks

The use of merchant velocity checks, if available, to track the number of transactions associated with the same credit or debit card within a specific timeframe in the merchant's system, is often useful in identifying fraudulent activity. Velocity checking allows a merchant to identify how many times a customer has used the same card at the store location(s), and highlight excessive transaction activity. Excessive transaction activity may not necessarily be an indication of fraud; however, merchant awareness could potentially lessen the opportunity for fraud or allow for additional verification steps to be performed.

Merchants are advised to check with their acquirers on the availability of velocity checking.

3.1.4 Establish a Strategy for Transactions That Could Involve Counterfeit

Understanding the types of transactions that are being charged back due to network liability shifts can help merchants to take steps to reduce not only the risk of chargebacks but of fraud generally. As noted above, although the best solution to avoiding loss through CLS chargebacks is to become EMV enabled, taking appropriate steps in the interim will help reduce the likelihood and frequency of fraud and associated losses.

For example, merchants can review chargebacks to identify the kinds of goods or services or locations that are being targeted by fraudsters. Depending on the merchant, gift cards, electronics, cosmetics and other high end merchandise are often common fraud targets. By implementing internal procedures to address common fraud targets, merchants can help discourage attempted fraud in their own business.

Merchants are also encouraged to implement and inform staff of special procedures for transactions involving goods and services that are commonly targeted by fraudsters, and the reasons those transactions may be more closely monitored.

Additional simple measures include using a store manager or specific terminal to process gift card purchases above a specific dollar amount set by the merchant or to process transactions with large numbers of items. Merchants can also contact issuers to approve specific high risk transactions and/or to confirm cardholders; it is important to ensure that the actual issuing financial institution was contacted and some verification of cardholder identity takes place.

3.1.5 Implement PIN Prompting for Debit Transactions

To reduce fraud in merchant environments which have not yet moved to chip, consider PIN prompting for all PIN-capable debit transactions. Capturing a knowledge-based verification method at the point of sale can reduce fraud substantially. Merchants should also more heavily scrutinize transactions where the PIN prompt is bypassed above the no CVM limit. Additional information on CLS chargebacks for PIN-capable transactions is included in Section 7.

3.2 Merchants Who Are Chip-Enabled

Merchants who are chip-enabled can take several steps to avoid chargebacks.

3.2.1 Fallback

Merchants with EMV terminals should see higher rates of approvals on chip cards vs. magnetic stripe cards. Keeping terminals up to date with the software updates is essential to ensure these higher rates of approved transactions continue.

Once a merchant's EMV terminals are fully operational, a fallback transaction could be an indication that a fraudster has tampered with the chip or the magnetic stripe is counterfeit. Although the merchant is protected from the CLS chargeback when fallback occurs, a higher level of scrutiny should accompany any fallback to a magnetic stripe transaction. Merchants should not attempt to circumvent the chip card processes to trigger a magnetic stripe or key entered transaction.

Fallback based on improper POS Entry Mode and/or Terminal Entry Capability (TEC) value, stating the terminal is chip capable when it is not, has CLS chargeback implications for Accel® and MasterCard. For American Express, Discover, SHAZAM, and Visa, acquirers may be subject to compliance action. Accel and STAR Network acquirers may be subject to enforcement measures based on non-compliance of the technical specifications. AFFN, CU24, and NYCE debit networks use POS Entry Mode, Service Code and Terminal Entry Capability, to determine fallback and chargeback rights.

Critical values in the fallback process are shown in the table below.

Critical Values in the Fallback Compliance/Chargeback Process[8]	
Accel	Terminal Entry Capability (TEC); POS Entry Mode; Service Code
AFFN	POS Entry Mode; Service Code
American Express	POS Data Code; card service code
China UnionPay	POS Entry Mode; Terminal Entry Capability; Chip Condition Code
CU24	POS Entry Mode; Service Code
Discover	Terminal Entry Capability (TEC); POS Entry Mode; card service code
MasterCard	Terminal Capability; POS Entry Mode; Service Code; Data Element 55 data components
NYCE	POS Entry Mode; Service Code
PULSE	POS Entry Mode (to identify fallback transactions); Terminal Capability Indicator (to indicate the terminal as being chip-capable for PULSE transactions); Service Code
SHAZAM	Terminal Capability; Input Capability; POS Entry Mode; Service Code
STAR	POS Entry Mode; POS Condition Code
Visa	TEC; POS Entry Mode; Chip Service Code; chip data in Data Element 55/Field 55

3.2.2 PIN Support

For networks where LSLS chargebacks are a possibility, merchants are encouraged to certify online and offline PIN for both debit and credit. At a minimum, online PIN support is recommended to prevent LSLS chargebacks for U.S. debit cards for networks that have an LSLS, since debit cards are PIN-preferring on the U.S. common debit AID. Note: Merchants are not liable for LSLS chargebacks for transactions that qualify under the networks' No CVM required programs. Additional information on CLS chargebacks for PIN-capable transactions is included in Section 7.

[8] The table includes terminology specific to each network.

3.2.3 Data Quality

It is critical for merchants to maintain data integrity/accuracy across authorizations and settlement messages to alleviate confusion for issuers and minimize the chance for invalid chargebacks due to data quality.

Additional information on data quality is included in Section 6.

3.2.4 Partial Grade/Early Data Transactions[9]

All necessary data should be sent with the authorization request. Each network has its own rules for the data elements required in an authorization request message. Merchants should make themselves aware of those rules and work with their acquirers to ensure all required data is included in authorization messages. Once the terminal is identified as chip capable in the authorization request message, the CLS reason code for counterfeit chargeback is invalid for use by the issuer provided all the necessary chip data is passed through to the issuer.

A CLS chargeback and corresponding liability shift are based solely on the authorization data of the transaction. The authorization data cannot be corrected or altered to reverse a CLS chargeback from the merchant to the issuer.

[9] Partial grade/early data transactions were an early EMV implementation approach to encourage faster implementation prior to full issuer and acquirer host upgrades by not requiring the acquirer or issuer to provide and validate the full chip data.

4. Issuer Best Practices for Managing Disputes

4.1 Best Practices to Avoid Originating Invalid Chargebacks

4.1.1 Transaction Categories

As of the publication date of this document, CFLS applies only to counterfeit magnetic stripe transactions where the data originated from a contact or dual-interface chip card at attended and certain unattended (depending on the payment network) POS locations, that occur after the applicable liability shift date, and that are disputed by the cardholder.

4.1.2 Transactions that are Out of Scope for CLS Chargeback

Issuers are encouraged to ensure that their systems recognize the differences in the liability shift dates and the transaction types to which the liability shifts apply, as they relate to transactions conducted on cards in their portfolios. For example, automated fuel dispenser (AFD) and ATM transactions are out of scope until the relevant payment network liability shift dates go into effect.

In addition to transactions that occur at unattended AFD terminals or occur prior to the applicable liability shift date, or that the cardholder has not disputed, this section describes other transactions that are out of scope for CLS chargeback.

For additional information on liability shifts, see the U.S. Payments Forum white paper, "Understanding the 2015 U.S. Fraud Liability Shifts."[10]

4.1.2.1 Other Ineligible Transactions

The liability shifts do not apply to transactions on non-chip enabled cards; i.e., magnetic-stripe only cards. Please refer to each network's specifications for details on exact data fields/values that identify a card as chip-enabled. Chip cards can be identified by issuers using the Service Code field with a first byte value of 2 or 6.

In addition, certain payment networks have announced temporary changes in chargeback policies affecting low-value transactions and the number of transactions that can be charged back per card.[11,12] Issuers, merchants and acquirers should contact the payment networks to understand current policies.

4.1.2.2 Mobile and Other Tokenized Contactless Transactions

The liability shifts covered by this white paper do not apply to tokenized transactions (e.g., Apple Pay), originating from mobile payment devices that have been fraudulently provisioned, as they are considered account takeover fraud.

Issuers are also reminded that:

- When initiating a chargeback for tokenized transactions using other reason codes, the primary account number (PAN) and token data are required.
- Acquirers may re-present tokenized transactions if they do not receive the token data in the chargeback.

[10] http://www.emv-connection.com/understanding-the-2015-u-s-fraud-liability-shifts/

[11] https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.2177933.html

[12] http://about.americanexpress.com/news/pr/2016/amex-updates-emv-fraud-policies.aspx

4.1.2.3 Other Transactions from Contact Chip-Enabled Terminals

Correctly processed transactions from contact chip-enabled terminals, regardless of POS entry mode (i.e., key entry, magnetic stripe, contact chip or contactless chip), are ineligible for counterfeit chargebacks under the U.S. EMV liability shift rules.[13] However, other chargeback rules may apply for key-entered transactions.

4.1.2.4 Fallback[14]

CLS chargebacks are applicable only when the technology of the chip card is greater than the technology of the terminal. If the terminal is chip enabled a chip card is presented at a properly configured terminal and the transaction falls back to magnetic stripe, the issuer will still maintain the liability for the transaction. For key entry, the issuer maintains CLS liability for the transaction for Accel, AFFN, CU24,MasterCard, NYCE, SHAZAM, the STAR Network and Visa, if all proper manual key entry procedures are followed and the authorization shows a properly operating chip terminal according to the network or brand terminal identification specifications.[15] For American Express and Discover, the acquirer/merchant maintains CLS liability for key entry.

4.2 Managing Cardholder Disputes of Transactions

In general, assuming the account is in good standing at the time of the transaction and regardless of the liability shift date or the POS entry mode, all network rules require that a transaction must be disputed by the cardholder as either counterfeit or lost/stolen prior to or on the date the issuer initiated a CLS chargeback.

As part of this process, the cardholder must clearly and correctly identify the fraudulent charges from the good charges. As important as identifying the fraudulent charges is that the cardholder is asked to confirm whether the card remains in their possession or whether the card was physically stolen and is no longer in the cardholder's possession. When a CLS dispute is started by the cardholder, the issuer has an obligation to mark the card account as compromised and issue a new card number and plastic card to the cardholder.

When a card is physically stolen, the fraudulent charges are more likely to be lost or stolen fraud, than counterfeit fraud. However, if the card is still in the cardholder's possession then it is very likely that account data has been compromised and the fraud is occurring on a counterfeit card(s).

Acquirers are urged to distinguish between the various network policies on liability shift. While the majority of networks have introduced counterfeit liability shift, not all networks support a lost and stolen liability shift. Furthermore, for the networks that support a lost and stolen liability shift, that shift only applies when PIN-preferring chip cards are used in merchant environments that either do not support chip, or support chip but do not support PIN. As a result, not all counterfeit, lost or stolen fraud is eligible for CLS chargeback, and it is critical that issuers fully understand the relevant network rules and policies prior to initiating CLS chargebacks.

From an issuing best practices standpoint, banks typically follow a regimen such as:

[13] Under American Express rules, the acquirer maintains CLS liability for key-entered transactions

[14] Additional information is available in the U.S. Payments Forum white paper, "EMV Implementation Guidance: Fallback Transactions," http://www.emv-connection.com/downloads/2012/05/Fallback-Transaction-Guidance-Final-Nov-2015.pdf

[15] Key entry transactions may be subject to chargeback based on factors outside of CLS. For guidance on manual key entry procedures, please refer to the relevant payment network documentation.

- Each individual fraud or potential fraud case is investigated and evaluated before any actions are taken. In no circumstances are automatic chargeback or automatic account charge-offs or closures put into place.
- Claims are segregated by varying attributes, such as type of risk associated with the claim and dollar amount. Then, upon segregation, claims are given to individuals that are specialists in a particular claim type.
- The fraud platform and the disputes and claims platforms are synchronized allowing the cardholder's account to be credited as soon as possible, facilitating a premium customer experience.
- Decisions are evaluated on customer relations with the bank, exposure amount, and network and regulatory chargeback rights.
- As in any circumstance, the related banking regulation is used as the ultimate guideline.

5. Merchant and Acquirer Best Practices for Disputing and Mitigating Chargebacks

There are a number of valid reasons an acquirer or merchant may re-present a CLS chargeback, including but not limited to the following:

- Invalid documentation
  - Where the cardholder fails to state that the card is in their possession (counterfeit CLS) or the card was lost or stolen (chip/PIN CLS) and not in their possession, if the network requires the information to be provided to the acquirer.
- The service code appearing in the authorization is not 2XX or 6XX.
  - This means the card was accepted at the point of interaction (POI) as a magnetic stripe card.
- The transaction was identified as an AFD in the authorization.
  - The chargeback is invalid until October 2017.
- The transaction was identified as a contactless transaction.
- Authorization data confirms both the card and the terminal were EMV enabled and valid data supports this fact.
- For lost/stolen, the 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.
- The transaction was not properly reported as fraud according to the brand or network CLS chargeback requirements.

When a CLS chargeback is valid, it is essential that the acquirer not re-present the chargeback. Invalid re-presentments, like invalid chargebacks, are costly to both the acquirer and issuer.

An issuer must provide supporting cardholder documentation with a fraud-related chargeback. If a CLS chargeback does not contain the required supporting cardholder information or is otherwise invalid, an acquirer can automatically respond on behalf of the merchant back to the issuer on the CLS chargeback.

Many merchants have deployed chip terminals in stages and use 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.

Data that merchants/acquirers should maintain to successfully re-present chargebacks include:

- For counterfeit: service code; issuer approval number; terminal entry capability; attended terminal status; evidence that chip data/Field 55 was sent; and POS entry mode
- For lost/stolen: service code; issuer approval number; terminal entry capability; attended terminal status; evidence that chip data/Field 55 was sent; terminal PIN pad status in data/field 55; terminal verification results (TVR); card verification results (CVR); POS entry mode; and POS PIN Entry Mode

Where these may reside in the message may vary by payment network; contact the acquirer for more information on network-specific message formats and data locations.

6. Data Quality, Authorization and Chargebacks

Despite following network requirements and best practices, data quality issues may contribute significantly to the occurrence of invalid CLS chargebacks. The following describes the most common and severe data quality problems.

6.1 Differing TEC Values

The authorization record contains data that indicates whether the terminal is contact chip enabled (the Terminal Entry Code (TEC)) and the settlement record for the transaction must contain the same TEC value. If the two values don't match, the data quality issue may result in erroneous chargeback reason codes by the issuer should a cardholder initiate a dispute. The following are examples of this issue:

- A transaction authorization record contains a TEC value indicating that the terminal is not contact-chip enabled, but the subsequent settlement/clearing record for the same transaction contains a TEC value which indicates that the terminal is contact chip-enabled.
- A transaction authorization record contains a TEC value that indicates a chip transaction, but the settlement/clearing record indicates the terminal is not contact chip enabled.

All authorization requests and clearing records must contain complete, accurate, and valid data. If an authorization is obtained, any data in the subsequent clearing record must be the same as, or consistent with, comparable data in the authorization request and authorization response.

7. Network Differences for Lost/Stolen CLS Chargebacks

For networks that do not support lost and stolen liability shift, only counterfeit fraud may be charged back.

For networks that do support lost or stolen liability shift, the cardholder must indicate the sale resulted from a lost/stolen, PIN-preferring card in order to issue a CLS chargeback for lost/stolen fraud and shift liability to the merchant. In addition, PIN (online or offline) must be higher priority than signature on the PIN-preferring chip card's Cardholder Verification Method (CVM) list and the merchant terminal did not have the ability to support PIN or did not have a working PIN pad at the time of the transaction. Assuming the terminal PIN pad is operational, the lost/stolen liability shift is not applicable if the properly operating chip terminal matches the highest priority CVM of the chip card.

Please note that the data in Data Element 55 must be reviewed for applicability of the code. Depending on the network, other data may be consulted as well to determine chargeback applicability. While indicators in the authorization message may show the merchant to be PIN enabled, the data within the Terminal Capabilities and Terminal Verification Results tag of Data Element/Field 55 will need to be reviewed to determine whether the lost/stolen liability shift applies. It is important to note that some terminals have been enabled for a phased implementation approach where EMV is supported for "credit" for the global networks and the U.S. common debit AID is not yet supported. Where the U.S. common debit AID is not supported, chip liability shifts applies if the transaction proceeds as a magnetic stripe transaction.[16]

Also, a PIN bypass may occur that causes the authorization to fallback to a signature CVM or No CVM. If Data Element/Field 55 confirms the PIN bypass and the issuer approves the authorization, then the issuer bears liability for the transaction. Please refer to the U.S. Payments Forum white paper on PIN bypass[17] for details on how and why PIN bypass occurs.

For further assistance, please see the examples below:

- Offline PIN-preferring card, terminal only supports online PIN (chip)

American Express	The issuer does not have a lost/stolen chargeback right. U.S. merchants must support PIN (online or offline) to obtain lost/stolen liability shift protection.
Discover	U.S. merchants supporting chip/PIN must support both online and offline PIN to avoid the lost/stolen liability shift.
MasterCard	The issuer potentially has a lost/stolen liability shift chargeback right. U.S. merchants supporting chip/PIN must support both online and offline PIN to help prevent the lost/stolen liability shift.
Visa	Visa does not have a lost/stolen liability shift in the U.S. The issuer does not have a lost/stolen chargeback right.

[16] The information provided pertains only to the payment networks participating in the document.

[17] "PIN Bypass in the U.S. Market, U.S. Payments Forum white paper, February 2016, http://www.emv-connection.com/pin-bypass-in-the-u-s-market/

- Offline or online PIN-preferring card, terminal supports magnetic stripe and online PIN

American Express	Not applicable. American Express does not support magnetic stripe PIN in the United States.
Discover	Lost/stolen liability shift does not apply if the online PIN is present in a transaction approved by the issuer. Merchants must support chip transactions to avoid counterfeit liability shift.
MasterCard	If the online PIN is approved, the lost/stolen liability shift does not apply to transactions with online PIN-preferring cards. The lost/stolen liability shift does potentially apply to transactions with offline PIN-preferring chip cards. Also, other dispute rights may exist for counterfeit-related fraud.
Visa	Visa does not have a lost/stolen liability shift in the U.S. The issuer does not have a lost/stolen chargeback right.

- Online PIN-preferring card, terminal supports only offline PIN (chip)

American Express	The issuer does not have a lost/stolen chargeback right. U.S. merchants must support PIN (online or offline) to obtain LSLS protection.
Discover	The issuer can initiate a lost/stolen liability shift chargeback. U.S. merchants supporting chip/PIN must support both online and offline PIN to avoid the lost/stolen liability shift.
MasterCard	The issuer potentially has a lost/stolen liability shift chargeback right. U.S. merchants supporting chip/PIN must support both online and offline PIN to help prevent the lost/stolen liability shift.
Visa	Visa does not have a lost/stolen liability shift in the U.S. The issuer does not have a lost/stolen chargeback right.

8. Conclusions

The issues surrounding liability shift, chargebacks and re-presentments are somewhat complex, but all hinge on the authorization process and data integrity. Most acquirer/merchant disputes of chargebacks are resolved between the issuer and acquirer/merchant. Where agreement cannot be reached, the final resolution rests with the network responsible for processing the transaction. In addition, data and evidence specific to each chargeback may be necessary to determine the final outcome in the dispute process.

Regardless, this white paper presents guidelines to avoid the issuance of invalid CLS chargebacks or in the event a CLS chargeback issued, best practices to mitigate against any invalid CLS chargeback. As issuer and merchant chip implementations become more robust and data quality improves, the occurrence of invalid CLS chargebacks is expected to decrease. More importantly, as the U.S. EMV migration progresses, the number of card-present disputes is expected to drop off as counterfeit fraud is reduced by EMV implementation. This is the ultimate goal of the U.S. migration to EMV and one on which issuers, merchants, networks and acquirers can all agree.

9. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the scenarios and payment networks specifically identified above, and that applicable rules, processing, liability and/or results may be impacted by specific facts or circumstances.

Additionally, each payment network determines its own rules, requirements, policies and procedures regarding liability, liability shifts, transaction processing and chargebacks, all of which are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with their respective payment networks regarding all applicable rules, requirements, policies and procedures.