Understanding the U.S. EMV Liability Shifts

Version 2.0

Date: July 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: info@uspaymentsforum.org.

Table of Contents

1. Introduction

EMV has been implemented in the United States, as it has in other countries, with the goal of reducing card-present fraud. Changes in payment network rules seek to support the migration to EMV by placing liability for fraud – counterfeit, and in the case of most networks, also lost or stolen – with the party to the transaction that has not successfully transitioned to EMV chip technology.

Most U.S. payment networks have implemented EMV fraud “liability shifts,” effective October 2015, for POS transactions. Some networks also have either implemented or announced liability shifts for ATMs and/or automated fuel dispensers (AFDs). With these liability shifts, many card issuers, merchants, acquirers and processors implementing EMV chip technology are asking, “Who is liable for what, and when, under these fraud liability shifts?” The U.S. Payments Forum is providing information collected from certain payment networks to help payment industry participants better understand the corresponding network’s policies. This document includes details for each of the networks specified below regarding their respective liability shifts for counterfeit and lost-or-stolen fraud, for POS devices, ATMs, and AFDs.[1]

Prior to these liability shifts taking effect, liability for card-present fraudulent transactions has generally been the responsibility of card issuers. These liability shifts apply to transactions from a counterfeit card created from copying magnetic stripe data from a chip card and/or from lost or stolen chip cards. As the various liability shift dates are reached, liability for those transactions generally shifts to the acquirer/merchant in certain cases if they do not use EMV chip-enabled[2] devices and applications to process payment transactions. The impact of these liability shifts to the acquirer/merchant depends on whether:

- EMV chip cards (domestic and international – including credit and debit cards) are used; and
- EMV chip-enabled acceptance devices/applications are deployed, including in-person POS retail devices, unattended terminals (including ATMs and AFDs), kiosks and vending machines, and mobile payment acceptance devices (MPOS)

2. Counterfeit Fraud Liability Shift Scope

The counterfeit card liability shift only pertains to transactions where a counterfeit magnetic stripe is presented to a POS terminal that does not support, at a minimum, contact chip EMV.

2.1 POS Counterfeit Fraud Liability Shifts

Applies to Accel, AFFN, American Express, China UnionPay, CU24, Discover, Mastercard, NYCE Payments Network, PULSE, SHAZAM Network, STAR Network and Visa

As of October 2015, for the payment networks noted immediately above, when a magnetic stripe card that was counterfeited with track data copied from an EMV chip card is swiped at a POS device/application that is not EMV chip-enabled, and the transaction is successfully processed, the acquirer/merchant may be liable for the chargeback resulting from any potential fraud.

[1] Note that information was validated at the time of publication and is subject to change. Merchants and acquirers are advised to consult with their respective payment networks regarding applicable liability shifts and rules.

[2] Chip-enabled device or terminal: A terminal that has, or is connected to, a contact chip card reader, has an EMV application, and is certified and able to process EMV transactions.

The POS counterfeit liability shifts for the above-listed networks for the U.S. are summarized in the following chart.

Chip Capability: Card	Chip Capability: POS	Counterfeit Liability after October 2015 Lies with:
Magnetic stripe only card	Terminal not enabled for contact chip	Issuer
Magnetic stripe only card	Contact-chip-enabled	Issuer
Chip card	Contact-chip-enabled	Issuer
Counterfeit magnetic stripe card with track data copied from a chip card[3]	Terminal not enabled for contact chip	Acquirer/Merchant
Counterfeit magnetic stripe card with track data copied from a chip card[3]	Contact-chip-enabled	Issuer[4]

Exceptions. Certain payment networks announced interim changes to the POS liability shift policies in mid-2016 to help reduce counterfeit fraud costs for merchants who have not yet upgraded their point-of-sale terminals to accept EMV chip cards. These changes include:

- Not holding merchants liable for counterfeit fraud when a transaction is under a set dollar amount.
- Limiting the number of counterfeit fraud transaction chargebacks per card account.

Merchants are advised to check with their acquirers and issuers are advised to check with their issuer processors or the payment networks for details on liability policies and timing of the policy changes.

See Section 4 for additional information for fallback transactions.

2.2 ATM Counterfeit Fraud Liability Shifts

Applies to Accel, AFFN, China UnionPay, CU24, Discover, Mastercard, NYCE Payments Network, PULSE, SHAZAM, STAR Network and Visa

Some networks have also implemented or announced a counterfeit liability shift for ATM transactions. The chart below summarizes the various ATM liability shifts for the networks listed.

Chip Capability: Card	Chip Capability: ATM	Counterfeit Liability
Magnetic stripe only card	Terminal not enabled for contact chip	Issuer: Accel, AFFN, China UnionPay, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa

[3] Data from a contact chip card.

[4] Counterfeit liability lies with issuer if the transaction is processed as fallback and approved by the issuer.

Chip Capability: Card	Chip Capability: ATM	Counterfeit Liability
Magnetic stripe only card	Contact-chip-enabled	Issuer: Accel, AFFN, China UnionPay, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa
Chip card	Contact-chip-enabled	Issuer: Accel, AFFN, CU24, Discover, Mastercard, NYCE, PULSE, STAR, Visa
Counterfeit magnetic stripe card with track data copied from a chip card[5]	Terminal not enabled for contact chip	Issuer: • Accel, AFFN, China UnionPay, CU24, NYCE, STAR, Visa (before Oct. 1, 2017) • Mastercard (before Oct. 1, 2016) • PULSE: Based on front-of-card brand's date ○ Before Oct. 1, 2017 – Issuer liability for PULSE cards cobranded with Mastercard ○ After Oct. 1, 2017 – Issuer liability / all brands • SHAZAM ○ Before Oct. 1, 2016 – Issuer liability with Mastercard co-branded cards ○ Before Oct. 1, 2017 – Issuer liability with Visa co-branded cards ATM acquirer: • Accel, AFFN, China UnionPay, CU24, NYCE, STAR, Visa (after Oct. 1, 2017) • Mastercard (after Oct. 1, 2016) • SHAZAM ○ MasterCard co-branded – after Oct. 1, 2016 ○ VISA co-branded – after Oct. 1, 2017
Counterfeit magnetic stripe card with track data copied from a chip card[5]	Contact-chip-enabled	Issuer: • Accel, AFFN, China UnionPay, CU24, Mastercard, Discover, NYCE, Visa, SHAZAM, STAR Network • PULSE: Based on front-of-card brand's date ○ Before Oct. 1, 2017 - Issuer liability for PULSE cards cobranded with Mastercard ○ After Oct. 1, 2017 – Issuer liability / all brands

2.3 AFD Counterfeit Fraud Liability Shifts

Applies to Accel, AFFN, American Express, CU24, Discover, Mastercard, NYCE Payments Network, PULSE, SHAZAM, STAR Network and Visa

Lastly, the networks identified above have also announced the counterfeit liability shifts for automated fuel dispensers. The chart below gives specific information for each of these networks regarding their AFD liability shifts.

[5] Data from a contact chip card.

Chip Capability: Card	Chip Capability: AFD	Counterfeit Liability
Magnetic stripe only card	Terminal not enabled for contact chip	Issuer: Accel, AFFN, American Express, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa
Magnetic stripe only card	Contact-chip-enabled	Issuer: Accel, AFFN, American Express, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa
Chip card	Contact-chip-enabled	Issuer: Accel, AFFN, American Express, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa
Counterfeit magnetic stripe card with track data copied from a chip card[6]	Terminal not enabled for contact chip	Domestic issuer: • Accel, AFFN, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa (before Oct. 1, 2020)* • American Express (before Oct. 16, 2020) International Issuer: • American Express (before Oct. 16, 2020) • STAR (before Oct. 1, 2020) Merchant/acquirer: • Accel, AFFN, CU24, Discover, Mastercard, NYCE, PULSE, Visa (after Oct. 1, 2020 for domestic issuer cards) • Mastercard, Visa (after Oct. 1, 2017 for international issuer cards (cross border)* • American Express (after Oct. 16, 2020) • SHAZAM, STAR (after Oct. 1, 2020)
Counterfeit magnetic stripe card with track data copied from a chip card[6]	Contact-chip-enabled	Issuer: Accel, AFFN, American Express, CU24, Discover, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa

**For American Express, Mastercard and Visa, AFD merchants may be liable for excessive fraud transactions under existing programs separate from the liability shift. Please contact your network representative for further information.*

Exceptions. There are some exceptions to these liability shifts. Merchants are advised to check with their acquirers and issuers are advised to check with their issuer processors or the payment networks for details on liability policies and timing of the policy changes.

[6] Data from a contact chip card.

3. Lost-or-Stolen Fraud Liability Shift for Contact Transactions

As of October 2015 for American Express, Discover and Mastercard, the acquirer/merchant may also be liable for a chargeback resulting from lost-or-stolen fraud on contact transactions if:

1. A PIN-preferring (either online or offline PIN) chip card that has been stolen (not a copy or counterfeit) is presented at a magnetic stripe-only POS device/application, and the stolen chip card is processed as a magnetic stripe transaction OR
2. A PIN-preferring (either online or offline PIN) chip card that has been stolen (not a copy or counterfeit) is presented at a chip-enabled merchant POS device/application that does not support either online or offline PIN, and the stolen chip card is processed as a signature chip transaction.

PIN Entry Bypass: In the case where PIN entry bypass[7] is invoked by the cardholder and is properly identified by the acquirer/merchant in the authorization message as specified by the EMV specification, liability stays with the issuer if the issuer approves the transaction. Other dispute rules may apply if PIN is bypassed using some other approach; additional details can be found in the U.S. Payments Forum white paper, "PIN Bypass in the U.S. Market."[8]

No CVM (Cardholder Verification Method) transactions that meet the No CVM requirements of the payment network are not affected by the EMV lost-or-stolen liability shift. Mastercard does not support the use of the lost-or-stolen chip liability shift for transactions performed at Cardholder Activated Terminals (CAT) Level 2 (online authorized with No CVM).

There is no lost-or-stolen liability shift for ATM.

3.1 POS Lost-or-Stolen Fraud Liability Shifts

The U.S. lost or stolen liability shifts for POS transactions are summarized in the following chart for the networks identified immediately below.

Applies to American Express, Discover and Mastercard

Chip & CVM Capability: Card	Chip & CVM Capability: POS	Lost/Stolen Liability after October 2015 Lies with:
Magnetic stripe card	Any terminal type	Issuer*
Chip card, PIN-preferring CVM (online or offline)	Terminal not enabled for contact chip	Acquirer/Merchant**
Chip card, signature-preferring CVM	Terminal not enabled for contact chip	Issuer***

[7] PIN entry bypass is an optional function in a traditional EMV environment that may be invoked when the following occurs: the CVM list of the selected AID has PIN as the preferred CVM for the given transaction and the terminal has a Terminal Capability indicator supporting "PIN;" the terminal prompts the cardholder for a PIN; and the cardholder does not enter the PIN and invokes this function.

[8] http://www.emv-connection.com/pin-bypass-in-the-u-s-market/

Chip & CVM Capability: Card	Chip & CVM Capability: POS	Lost/Stolen Liability after October 2015 Lies with:
Chip card, signature-preferring CVM	Contact-chip-enabled, signature CVM (no PIN capability)	Issuer
Chip card, PIN-preferring CVM (online or offline)	Contact-chip-enabled, signature CVM (no PIN capability)	Acquirer/Merchant
Chip card, signature-preferring CVM	Contact-chip-enabled, PIN CVM (online and/or offline)	Issuer
Chip card, PIN-preferring CVM (online or offline)	Contact-chip-enabled, PIN CVM (online and/or offline)****	Issuer

* *Magnetic stripe liability shift rules apply.*

** *If PIN was prompted and approved, magnetic stripe liability rules may apply. Refer to payment network rules for additional information.*

*** *Lost-or-stolen liability shift applies to only legitimate cards that are lost or stolen based on issuer determination.*

**** *Payment networks have slightly different policies. In the U.S. for MasterCard and Discover, if a merchant decides to support PIN, the terminal must support both online and offline PIN. In the U.S. for American Express, the merchant terminal can support either offline PIN, online PIN or both. In all three cases, the issuer retains liability if a fraudulent lost or stolen PIN-preferring chip card is used at a chip-enabled terminal that supports PIN.*

Applies to Accel, AFFN, China UnionPay, CU24, JCB, NYCE Payments Network, STAR Network and Visa

There is no change to Accel, AFFN, China Union Pay, CU24, JCB, NYCE, STAR Network or Visa liability for lost-or-stolen card fraud for contact transactions at the POS, and accordingly, this liability remains with the issuer.

3.2 AFD Lost-or-Stolen Fraud Liability Shift

The U.S. lost-or-stolen liability shifts for AFD transactions are summarized in the following chart for the networks identified immediately below.

Applies to American Express, Discover, Mastercard and PULSE

Chip & CVM Capability: Card	Chip & CVM Capability: AFD	Lost/Stolen Liability after October 2020 Lies with:
Magnetic stripe card	Any terminal type	Issuer*
Chip card, PIN-preferring CVM (online or offline)	Terminal not enabled for contact chip	Acquirer/Merchant**

Chip & CVM Capability: Card	Chip & CVM Capability: AFD	Lost/Stolen Liability after October 2020 Lies with:
Chip card, signature-preferring CVM	Terminal not enabled for contact chip	Issuer***
Chip card, signature-preferring CVM	Contact-chip-enabled, signature CVM (no PIN capability)	Issuer
Chip card, PIN-preferring CVM (online or offline)	Contact-chip-enabled, signature CVM (no PIN capability)	Acquirer/Merchant
Chip card, signature-preferring CVM	Contact-chip-enabled, PIN CVM (online and/or offline)	Issuer
Chip card, PIN-preferring CVM (online or offline)	Contact-chip-enabled, PIN CVM (online and/or offline)****	Issuer
Chip card, PIN-preferring CVM (online or offline)	Contact-chip-enabled, No CVM	Issuer (Mastercard)
Chip card, signature-preferring	Contact-chip-enabled, No CVM	Issuer (Mastercard)
Magnetic stripe card	Contact-chip-enabled, No CVM	Issuer (Mastercard)

* *Magnetic stripe liability shift rules apply.*

** *If PIN was prompted and approved, magnetic stripe liability rules may apply. Refer to payment network rules for additional information.*

*** *Lost-or-stolen liability shift applies to only legitimate cards that are lost or stolen based on issuer determination.*

**** *Payment networks have slightly different policies. In the U.S. for MasterCard and Discover, if a merchant decides to support PIN, the terminal must support both online and offline PIN. In the U.S. for American Express, the merchant terminal can support either offline PIN, online PIN or both. In all three cases, the issuer retains liability if a fraudulent lost or stolen PIN-preferring chip card is used at a chip-enabled terminal that supports PIN.*

For Visa, as of 15 April 2014, lost-or-stolen liability at the AFD lies with the issuer on EMV chip transactions conducted as No CVM, as long as a full strength EMV cryptogram is presented with all related chip data.

Applies to Accel, AFFN, JCB and STAR Network

There is no change to Accel, AFFN, and STAR Network liability for lost-or-stolen card fraud for contact AFD transactions, and accordingly, this liability remains with the issuer.

4. Technical Fallback and Manual Key Entry

For fallback transactions,[9] excluding manual key entry, as long as the acquirer/merchant sends the appropriate indicators identifying the transaction as fallback, the issuer bears the liability if they approve the fallback transaction. However, fallback rates that exceed the acceptable thresholds set by the payment networks for fallback that results from other exceptions may result in other impacts to the acquirers/merchants as determined by those payment networks.

If the magnetic stripe of a chip card cannot be read, transactions may be completed at a terminal using PAN key entry. Certain payment networks may not require the support of manual key entry for chip or magnetic stripe cards anymore; if the merchant uses manual key entry, the merchant is liable for fraudulent transactions.

Some payment networks have also introduced new rules to discontinue the use of the card security code (e.g., CVV2/CVC2) with electronically read card-present transactions, or manual key-entered transactions.

Please contact the payment networks for additional information on their policies for fallback and key-entered transactions.

5. Liability Shifts for Cross-Border Transactions[10]

It is important to understand for each payment network the consistencies in liability shifts for cross-border transactions. This section describes liability shifts for U.S. acquirers/merchants when non-U.S.-issued cards are used at U.S. merchants and liability shifts when U.S.-issued cards are used at non-U.S merchants.

Counterfeit Liability Shift. For the global payment networks listed in the counterfeit liability shift fraud section above (American Express, China UnionPay, Discover, MasterCard and Visa), their respective counterfeit liability shifts are consistent for all cross-border POS, ATM and AFD transactions for participating countries in the EMV liability shift. For Accel cross-border transactions initiated with Canadian issuer cards participating in Accel, the liability shift is consistent with POS and ATM transaction policies effective October 1, 2020.

Lost-or-Stolen Liability Shift. In countries where American Express, Discover, MasterCard and Visa have lost-or-stolen liability shift policies for POS and AFD transactions, for cross-border transactions, the policy of the country with the weakest liability policy will govern the transaction. For instance, if a card from a country with a lost-or-stolen liability shift is used at a terminal in a country that does not have the liability shift, then the transaction is not subject to a lost-or-stolen chargeback. For the global payment networks listed above that do not have a U.S. lost-or-stolen liability shift (China UnionPay, JCB), lost-or-stolen liability shift on cross-border transactions does not apply even if the card-issuer's country has implemented a lost-or-stolen liability shift.

[9] Fallback transaction: A transaction that is initiated between a chip card and a chip terminal but chip technology is not used and the transaction is completed via magnetic stripe. See additional information on fallback transactions in the U.S. Payments Forum white paper, "EMV Implementation Guidance: Fallback Transactions," http://www.uspaymentsforum.org/emv-implementation-guidance-fallback-transactions/.

[10] Cross-border transaction: A transaction where a card issued in one country is used for a payment transaction in a different country.

6. Mobile and Contactless Transactions

As contactless adoption accelerates in the U.S., it is important for merchants and issuers to stay current on potential global network policy changes that govern mobile and contactless EMV transactions.

Most networks do not have a counterfeit liability shift for contactless transactions in the U.S. Merchants should not expect to receive counterfeit chargebacks on contactless transactions. However, if a merchant does not support contact chip, they may still be held liable for counterfeit magnetic stripe fraud perpetrated using a mobile device.

For certain networks, issuers are also reminded that, per network rules:

- 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.

Applies to American Express and Discover

For the global networks in the U.S. that have lost-or-stolen fraud liability shift policies, those policies continue to apply to contact EMV transactions only and not to mobile EMV or contactless EMV transactions.

Applies to Mastercard

In any scenario where a secure contactless CVM (online PIN or CDCVM[11]) was actually used, lost-or-stolen liability shift does not apply. For example, if both the card and POS terminal support online PIN and this was used, the issuer cannot charge back a transaction because the terminal did not support CDCVM. This is true even if the terminal did not use MCL version 3.0 or 3.1 and/or was not configured to support CDCVM, but the Issuer Application Data carried in data element (DE) 55 (Integrated Circuit Card [ICC] System-related Data) confirms that CDCVM was completed.

7. Conclusion

This document summarizes, as of the publication date, the chip counterfeit as well as lost-or-stolen liability shifts which started in October 2015 in the United States across POS, ATM and AFD acceptance environments. Certain scenarios, such as merchant force post processing[12] and voice authorization, are not impacted by the liability shifts described above, and liability in those situations remains unchanged.

When considering the respective liability shifts described above, it helps to first define the *type* of fraud, and then assess the technology being employed by the applicable parties in light of applicable payment network rules. In summary, the party supporting the superior technology for each fraud type will prevail in a chargeback (for the scenarios specifically addressed above and except as otherwise noted); and in case of a technology tie, the fraud liability is generally unchanged and remains as it is today – with the issuer.

[11] Consumer Device Cardholder Verification Method. A type of CVM supported by the payment networks when assessing transactions originating from mobile devices.

[12] For additional information, see the U.S. Payments Forum “Merchant Processing during Communications Disruptions,” white paper, http://www.emv-connection.com/merchant-processing-during-communications-disruption/.

8. Legal Notice

There are additional scenarios that could affect liability that are not covered in this document, and the payment networks named above do not reflect all of the networks that may have liability shifts, but rather the ones that provided information to the U.S. Payments Forum in the preparation of this document. Additionally, certain networks identified above only provided information regarding liability shifts for counterfeit cards (not for lost or stolen cards).

Notwithstanding anything to the contrary in this document, each payment network determines its own policies and practices (including but not limited to rules regarding liability and timing of the liability shifts), all such policies and practices are subject to change, and liability in scenarios and/or for payment networks not specifically addressed above may differ.

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

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.