Understanding Fraud Liability for EMV Contact and Contactless Transactions in the U.S.

Version 3.0

Date: February 2019

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. The liability policies documented in this white paper were developed by the payment networks independently and provided to the Forum to summarize the policies for industry stakeholders. 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)

The version 3.0 white paper includes expanded content on counterfeit and lost-or-stolen fraud liability for contactless transactions.

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.

[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.

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 presented 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.

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]

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.

See Section 4 for additional information for fallback transactions and Section 2.3 for AFD liability shifts.

2.2 ATM Counterfeit Fraud Liability Shifts

Applies to Accel, AFFN, China UnionPay, CU24, Mastercard, NYCE Payments Network, PULSE[5], 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, 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.

[5] Discover ATM fraud liability shift policies are managed by PULSE.

Chip Capability: Card	Chip Capability: ATM	Counterfeit Liability
Magnetic stripe only card	Contact-chip-enabled	Issuer: Accel, AFFN, China UnionPay, CU24, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa
Chip card	Contact-chip-enabled	Issuer: Accel, AFFN, CU24, Mastercard, NYCE, PULSE, STAR, Visa
Counterfeit magnetic stripe card with track data copied from a chip card[6]	Terminal not enabled for contact chip	ATM acquirer: Accel, AFFN, China UnionPay, CU24, Mastercard, NYCE, PULSE, SHAZAM, STAR, Visa
Counterfeit magnetic stripe card with track data copied from a chip card[5]	Contact-chip-enabled	Issuer: Accel, AFFN, China UnionPay, CU24, Mastercard, NYCE, PULSE, SHAZAM, STAR Network, Visa

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.

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[7]	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)

[6] Data from a contact chip card.

[7] Data from a contact chip card.

Chip Capability: Card	Chip Capability: AFD	Counterfeit Liability
		• 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.

3. Lost-or-Stolen Fraud for Face-to-Face Contact Transactions

As of October 2015 for American Express, Discover, Mastercard and PULSE, 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[8] 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."[9]

[8] 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.

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

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, Mastercard and PULSE

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***
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. This table assumes that the AFD terminal is online-capable.

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 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.*

Applies to Accel, NYCE, AFFN, JCB and STAR Network

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

3.3 Lost-or-Stolen Liability for Visa Including AFD and UCAT

3.3.1 Lost-or-Stolen Liability - Face-to-Face Environment

For Visa in the U.S. there is never any lost and stolen liability for the acquirer/merchant on electronic-read transactions in the face-to-face (F2F) environment. This is true regardless of whether the merchant has implemented EMV or not, and also true for both contact and contactless transactions.

3.3.2 Lost-or-Stolen Liability - Unattended Customer Activated Terminal (UCAT) Environment (Excluding AFD)

The unattended environment is slightly different for Visa. As with the F2F environment there is no lost-or-stolen liability for transactions below the Visa Easy Payment Service (VEPS) limit at qualified unattended devices. This is true regardless of whether the merchant has implemented EMV or not, and also true for both contact and contactless devices.

In 2014, Visa introduced a global reverse liability shift for chip transactions at unattended devices. Liability for lost-or-stolen that previously resided with the acquirer, at online capable unattended terminals, has been shifted back to the issuer for EMV chip-on-chip transactions, as long as a full strength cryptogram is presented with all related chip data.

Lost-or-stolen liability on magnetic stripe transactions, including MSD contactless and magnetic stripe fallback above the VEPS limit remains with the acquirer as before. Where possible, and at the discretion of the merchant, customers may be directed to pay at an attended kiosk to reduce the likelihood of fraud and avoid any possible liability on lost-or-stolen cards.

3.3.3 Lost-or-Stolen Liability - AFD Environment

There is generally no VEPS limit for AFD, however AFDs do qualify for relief from lost-or-stolen liability based on the same 2014 global reverse liability shift for chip transactions. For Visa, as of 15 April 2014, lost-or-stolen liability at the AFD lies with the issuer on EMV chip transactions for all CVMs, regardless of the AFD CVM capability, as long as a full strength EMV cryptogram is presented with all related chip data.

Lost-or-stolen liability on magnetic stripe transactions, including contactless magnetic stripe data and magnetic stripe fallback remains with the acquirer. Visa encourages merchants to use address verification and Visa Transaction Advisor on these transactions. Furthermore, customers may be directed to pay inside the convenience store to reduce the likelihood of fraud and avoid any possible liability on lost-or-stolen cards.

4. Technical Fallback and Manual Key Entry

For in-store fallback transactions,[10] 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. For AFD fallback transactions, 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, except for lost-or-stolen Visa transactions.[11] It is also important to note that 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[12]

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

[10] 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/.

[11] In the AFD environment, merchants may be liable for fallback transactions in lost-or-stolen cases for Visa. Visa advises that, where possible, magnetic stripe transactions on unattended chip terminals should be directed to pay inside.

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

payment networks listed above that do not have a U.S. lost-or-stolen liability shift (Visa, 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.

6. 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 contactless 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 any form factor, including contactless devices.

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.

6.1 Counterfeit Liability and Contactless Transactions

Counterfeit liability for contactless transactions is summarized in the following table for the networks identified. Three terminal capability scenarios are presented:

- Merchant terminal is enabled for EMV contactless and contact.
- Merchant terminal is enabled for magnetic stripe data (MSD) contactless and EMV contact.
- Merchant terminal is enabled for MSD contactless and not enabled for EMV contact.

Note that the liability information in this table is only valid if the transaction is properly identified based on payment network rules and the transaction is well-formed. Please consult with the payment networks for specifications.

Table 1. Counterfeit Liability for Contactless Transaction Scenarios for Identified Networks

	Scenario 1: Merchant terminal is enabled for EMV contactless and contact. *If the merchant is EMV enabled for contactless and contact, is the merchant ever liable for counterfeit contactless transactions? Does this change whether a contactless card, mobile phone with certified app*, or a mobile phone with rogue application is used?*	**Scenario 2: Merchant terminal is enabled for MSD contactless and EMV contact.** *If the merchant is MSD enabled for contactless and EMV for contact, is the merchant ever liable? Does this change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used?*	**Scenario 3: Merchant terminal is enabled for MSD contactless and not enabled for EMV contact.** *If the merchant is MSD enabled for contactless and not enabled for EMV contact, is the merchant ever liable? Does this change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used?*
Visa	No. As long as the merchant is enabled for contact EMV, TEC of 5, the merchant is always protected against counterfeit liability regardless of interface.	No. As long as the merchant is enabled for contact EMV, TEC of 5, the merchant is always protected against counterfeit liability regardless of interface. However, MSD must be removed by April 2019.	Yes. The merchant is liable for counterfeit fraud which is invariably going to take place via a magnetic stripe swipe, but could also take place using other contactless attack vectors. Acquirers are also reminded that MSD must be removed by April 2019.

	<u>Scenario 1</u>: **Merchant terminal is enabled for EMV contactless and contact.** *If the merchant is EMV enabled for contactless and contact, is the merchant ever liable for counterfeit contactless transactions? Does this change whether a contactless card, mobile phone with certified app*, or a mobile phone with rogue application is used?*	<u>Scenario 2</u>: **Merchant terminal is enabled for MSD contactless and EMV contact.** *If the merchant is MSD enabled for contactless and EMV for contact, is the merchant ever liable? Does this change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used?*	<u>Scenario 3</u>: **Merchant terminal is enabled for MSD contactless and not enabled for EMV contact.** *If the merchant is MSD enabled for contactless and not enabled for EMV contact, is the merchant ever liable? Does this change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used?*
Discover	No. The merchant is not liable for counterfeit contactless transactions. Discover's EMV fraud liability shift policy does not apply to contactless transactions.	No. The merchant is not liable for counterfeit contactless transactions. Discover's EMV fraud liability shift policy does not apply to contactless transactions.	No. The merchant is not liable for counterfeit contactless transactions. Discover's EMV fraud liability shift policy does not apply to contactless transactions.
PULSE	No. The merchant is not liable for counterfeit contactless transactions. PULSE's EMV fraud liability shift policy does not apply to contactless transactions.	No. The merchant is not liable for counterfeit contactless transactions. PULSE's EMV fraud liability shift policy does not apply to contactless transactions.	No. The merchant is not liable for counterfeit contactless transactions. PULSE's EMV fraud liability shift policy does not apply to contactless transactions.
NYCE	No. The merchant is not liable for EMV contactless transactions.	No. The merchant is not liable if the merchant is enabled for EMV.	Yes, If the payment method device is EMV capable (card or app) as defined in the track data within the message to the network.
UnionPay	No. If the issuer approves the transaction, the liability is to the issuer	N/A**	N/A**
CULIANCE	No. The merchant is not liable for counterfeit contactless transactions. No. It does not change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used.	No. The merchant is not liable. No. It does not change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used.	No. If the merchant is MSD enabled for contactless and not enabled for EMV contact, the merchant is not liable. No. It does not change whether a contactless card, mobile phone with certified app, or a mobile phone with rogue application is used.
Mastercard	No, as long as transaction properly coded as contactless	No, as long as transaction properly coded as contactless. However, this configuration is not valid based on existing Mastercard rules.***	No, as long as transaction properly coded as contactless
JCB	No. JCB does not have a contactless liability shift.	No. JCB does not support MSD contactless.	JCB does not support MSD contactless. If a JCB contact chip card is presented and the merchant is not EMV enabled, the merchant will be liable after October 1, 2019.
AFFN	No. Contactless card or in-app issuer is liable. This does not change based on application.	The merchant is not liable. The card or in-app issuer is liable. This does not change with application.	Yes. MSD Contactless Terminal: - MSD card or in-app, issuer liable - EMV contactless card or in-app, merchant liable
American Express	No. American Express EMV fraud liability shift does not apply to contactless	No. American Express EMV fraud liability shift does not apply to contactless	No. The merchant is not liable as American Express EMV fraud liability shift does not apply to contactless.

* A "certified app" is defined as an app like Apple Pay, Samsung Pay, Google Pay.

** UnionPay does not support MSD. UnionPay doesn't have MSD cards and doesn't support an app with MSD.

*** Mastercard does not allow EMV contact with MSD contactless terminals.

6.2 Lost-or-Stolen Liability and Contactless Transactions

Lost-or-stolen liability for contactless transactions is summarized in the following table for the networks identified. Three terminal capability scenarios are presented, with liability shown for transactions that are under and over the cardholder verification method (CVM) limit:

- Merchant terminal is enabled for magnetic stripe data (MSD) contactless and EMV contact.
- Merchant terminal is enabled for MSD contactless and not enabled for EMV contact.
- Merchant terminal is enabled for EMV contactless and contact.

Tables for both face-to-face POS transactions and unattended terminal transactions are shown. Note that information for Visa's lost-or-stolen liability is included in Section 3.3.

Table 2. Lost-or-Stolen Liability for Contactless Face-to-Face POS Transactions for Identified Networks

Face-to-Face POS Transactions	**Lost-or-Stolen Transaction Liability**	**Contactless MSD Mode Terminal on EMV Contact Terminal**		**Contactless MSD Mode Terminal on non-EMV Terminal**		**Contactless EMV Mode Terminal**	
		Under CVM Limit Transaction	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**
Discover*	MSD Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
	EMV Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
PULSE	MSD Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
	EMV Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer

Face-to-Face POS Transactions	**Lost-or-Stolen Transaction Liability**	**Contactless MSD Mode Terminal on EMV Contact Terminal**		**Contactless MSD Mode Terminal on non-EMV Terminal**		**Contactless EMV Mode Terminal**	
		Under CVM Limit Transaction	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**
NYCE**	MSD Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
	EMV Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
UnionPay	MSD Contactless Mode Payment Device	N/A	N/A	N/A	N/A	N/A	N/A
	EMV Contactless Mode Payment Device	N/A	N/A	N/A	N/A	Issuer	Issuer, if transaction approved
Mastercard	MSD Contactless Mode Payment Device	Issuer, considering transaction properly coded as contactless.	Issuer, if CVM properly processed. If terminal doesn't support online pin or CD-CVM, the merchant could be liable.	Issuer, considering transaction properly coded as contactless.	Issuer, if CVM properly processed. If terminal doesn't support online pin or CD-CVM, the merchant could be liable.	Issuer, considering transaction properly coded as contactless.	Issuer, if CVM properly processed. If terminal doesn't support online pin or CD-CVM, the merchant could be liable.
	EMV Contactless Mode Payment Device	Issuer, considering transaction properly coded as contactless.	Issuer, if CVM properly processed. If terminal doesn't support online pin or CD-CVM, the merchant could be liable.	Issuer, considering transaction properly coded as contactless.	Issuer, if CVM properly processed. If terminal doesn't support online pin or CD-CVM, the merchant could be liable.	Issuer, considering transaction properly coded as contactless.	Issuer, if CVM properly processed. If terminal doesn't support online pin or CD-CVM, the merchant could be liable.

Face-to-Face POS Transactions	**Lost-or-Stolen Transaction Liability**	**Contactless MSD Mode Terminal on EMV Contact Terminal**		**Contactless MSD Mode Terminal on non-EMV Terminal**		**Contactless EMV Mode Terminal**	
		Under CVM Limit Transaction	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**
JCB***	MSD Contactless Mode Payment Device	N/A	N/A	N/A	N/A	N/A	N/A
	EMV Contactless Mode Payment Device	N/A	N/A	N/A	N/A	Issuer	Issuer
AFFN	MSD Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
	EMV Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
American Express	MSD Contactless Mode Payment Device	N/A	N/A	N/A	N/A	N/A	N/A
	EMV Contactless Mode Payment Device	N/A Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	N/A Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	N/A Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	N/A Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer	Issuer

* Discover EMV fraud liability shift (FLS) is not applicable for contactless.

** NYCE Payment Network does not have a liability shift for lost or stolen.

*** JCB does not have a contactless or lost-or-stolen liability shift and does not support MSD contactless

Table 3. Lost-or-Stolen Liability for Contactless Unattended POS Transactions for Identified Networks

Unattended POS Transactions	**Lost-or-Stolen Transaction Liability**	**Contactless MSD Mode Terminal on EMV Contact Terminal**		**Contactless MSD Mode Terminal on non-EMV Terminal**		**Contactless EMV Mode Terminal**	
		Under CVM Limit Transaction	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**
Discover*	MSD Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
	EMV Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
PULSE	MSD Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
	EMV Contactless Mode Payment Device	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer
JCB**	MSD Contactless Mode Payment Device	N/A	N/A	N/A	N/A	N/A	N/A
	EMV Contactless Mode Payment Device	N/A	N/A	N/A	N/A	N/A	N/A
UnionPay	MSD Contactless Mode Payment Device	N/A	N/A	N/A	N/A	N/A	N/A
	EMV Contactless Mode Payment Device	N/A	N/A	N/A	N/A	Issuer	Issuer if transaction was approved

Unattended POS Transactions	**Lost-or-Stolen Transaction Liability**	**Contactless MSD Mode Terminal on EMV Contact Terminal**		**Contactless MSD Mode Terminal on non-EMV Terminal**		**Contactless EMV Mode Terminal**	
		Under CVM Limit Transaction	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**
American Express	MSD Contactless Mode Payment Device	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.
	EMV Contactless Mode Payment Device	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.	Issuer American Express EMV fraud liability shift does not apply to contactless or MSD.
Mastercard	MSD Contactless Mode Payment Device	Issuer, considering transaction properly coded as contactless.	Issuer, considering transaction properly coded as contactless and with correct CAT level information and CVM processed as required for the CAT level. Acquirer is responsible for contactless over CVM limit unless obtain PIN	Issuer, considering transaction properly coded as contactless.	Issuer, considering transactions properly coded as contactless and with correct CAT level information and CVM processed as required for the CAT level. Acquirer is responsible for contactless over CVM limit unless obtain PIN	Issuer, considering transaction properly coded as contactless.	Issuer, considering transaction properly coded as contactless and with correct CAT level information and CVM processed as required for the CAT level. Acquirer is responsible for contactless over CVM limit unless obtain PIN
	EMV Contactless Mode Payment Device	Issuer, considering transaction properly coded as contactless.	Issuer, considering transaction properly coded as contactless and with correct CAT	Issuer, considering transaction properly coded as contactless.	Issuer, considering transactions properly coded as contactless and with correct CAT	Issuer, considering transaction properly coded as contactless.	Issuer, considering transaction properly coded as contactless and with correct CAT

Unattended POS Transactions	**Lost-or-Stolen Transaction Liability**	**Contactless MSD Mode Terminal on EMV Contact Terminal**		**Contactless MSD Mode Terminal on non-EMV Terminal**		**Contactless EMV Mode Terminal**	
		Under CVM Limit Transaction	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**	**Under CVM Limit Transaction**	**Over CVM Limit Transaction**
			level information and CVM processed as required for the CAT level. Acquirer is responsible for contactless over CVM limit unless obtain PIN.		level information and CVM processed as required for the CAT level. Acquirer is responsible for contactless over CVM limit unless obtain PIN.		level information and CVM processed as required for the CAT level. Acquirer is responsible for contactless over CVM limit unless obtain PIN or CDCVM.

* Discover EMV fraud liability shift (FLS) is not applicable for contactless.

** JCB does not have a contactless or lost-or-stolen liability shift and does not support MSD contactless

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[13] 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.

The version 3.0 white paper expands the discussion of counterfeit and lost-or-stolen fraud liability for contactless transactions for the payment networks noted in Section 6.

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

[13] 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.