# Understanding the 2015 U.S. Fraud Liability Shifts

*Version 1.0 – May 2015*

Some U.S. payment networks are implementing EMV fraud "liability shifts" effective October 2015. With these liability shifts fast approaching, 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 EMV Migration Forum is providing this information collected from certain payment networks to help payment industry participants better understand the corresponding network's policies.

Today, across payment networks, liability for card-present fraudulent transactions is generally the responsibility of card issuers. Beginning in October 2015, certain U.S. payment networks independently plan to implement fraud liability shifts that will impact transactions from a counterfeit card created from the magnetic stripe on a chip card and/or lost or stolen card transactions. As of that date, liability for those transactions generally will shift to the acquirer/merchant in certain cases if they do not use EMV chip-enabled[1] devices and applications to process payment transactions. The impact of these October 2015 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 point-of-sale (POS) card payment acceptance devices/applications are deployed (excluding automated teller machines (ATMs) and automated fuel dispensers (AFDs)), including in-person POS retail devices, unattended terminals, kiosks and vending machines, and mobile payment acceptance devices (MPOS).

*ATMs and AFDs*: Liability shifts impacting ATMs and automated fuel dispensers have different timeframes and are not addressed in this document.

*Fallback Transactions*: For fallback transactions[2], as long as the acquirer/merchant sends the appropriate indicators identifying the transaction as fallback, the issuer will bear the liability if they approve the fallback transaction. However, fallback rates that exceed the acceptable thresholds set by the payment networks may result in other impacts to the acquirers/merchants as determined by those payment networks.

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

[2] 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.

## Counterfeit Fraud Liability Shift

***Applies to Accel, American Express, China UnionPay, Discover, MasterCard, NYCE Payments Network, SHAZAM Network, STAR Network and Visa***

Beginning in October 2015 for the nine payment networks noted immediately above, when a merchant accepts a magnetic stripe card that was counterfeited with track data copied from an EMV chip card, and the card is subsequently 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 the fraud.

The above counterfeit card liability shift only pertains to transactions where the magnetic stripe was read and does not apply to contactless transactions.

There is no anticipated liability shift for fallback transactions, as they are a result of the chip on the card not being read and the authorization message does not contain chip data. Fallback transactions are therefore considered magnetic stripe transactions and liability remains with the card issuer.

The 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 |

## Lost or Stolen Fraud Liability Shift

***Applies to American Express, Discover and MasterCard***

Beginning in October 2015 for American Express, Discover and MasterCard, the acquirer/merchant may also be liable for a chargeback resulting from fraud 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

[3] Data from a contact chip card.

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.

These lost or stolen liability shifts for the U.S. are summarized in the following chart:

| **Chip Capability: Card** | **Chip 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 apply.*

*** *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*.

*PIN Entry Bypass*: In the case where PIN entry bypass is invoked 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.

***Applies to Accel, China UnionPay, NYCE, STAR Network and Visa***
There is no expected change to Accel, China Union Pay, NYCE, STAR Network or Visa liability for lost or stolen card fraud, and accordingly, this liability remains with the issuer.

## Liability Shifts for Cross-Border Transactions[4]

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

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

counterfeit liability shift is consistent for all cross-border POS transactions for participating countries in the EMV liability shift.

***Lost-or-Stolen Liability Shift***. In countries where American Express, Discover and MasterCard have lost-or-stolen liability shift policies, their respective policies are consistent for domestic and cross-border transactions. For the global payment networks listed above that do not have a U.S. lost-or-stolen liability shift (China UnionPay and Visa), 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.

## Conclusion

This document summarizes, as of the publication date, the anticipated October 2015 U.S. liability shifts of the payment networks noted above in the specific scenarios described above. Certain scenarios, such as merchant stand-in and voice authorization, are not impacted by the October 2015 liability shifts described above, and liability in those situations is expected to remain as it is today.

When considering the October 2015 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 as of October 2015 generally is expected to remain as it is today – with the issuer.

## 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 October 2015 liability shifts, but rather the ones that provided information to the EMV Migration 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.

## About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the EMV chip implementation steps required for payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure chip technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate

successfully to chip technology in the United States. For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/