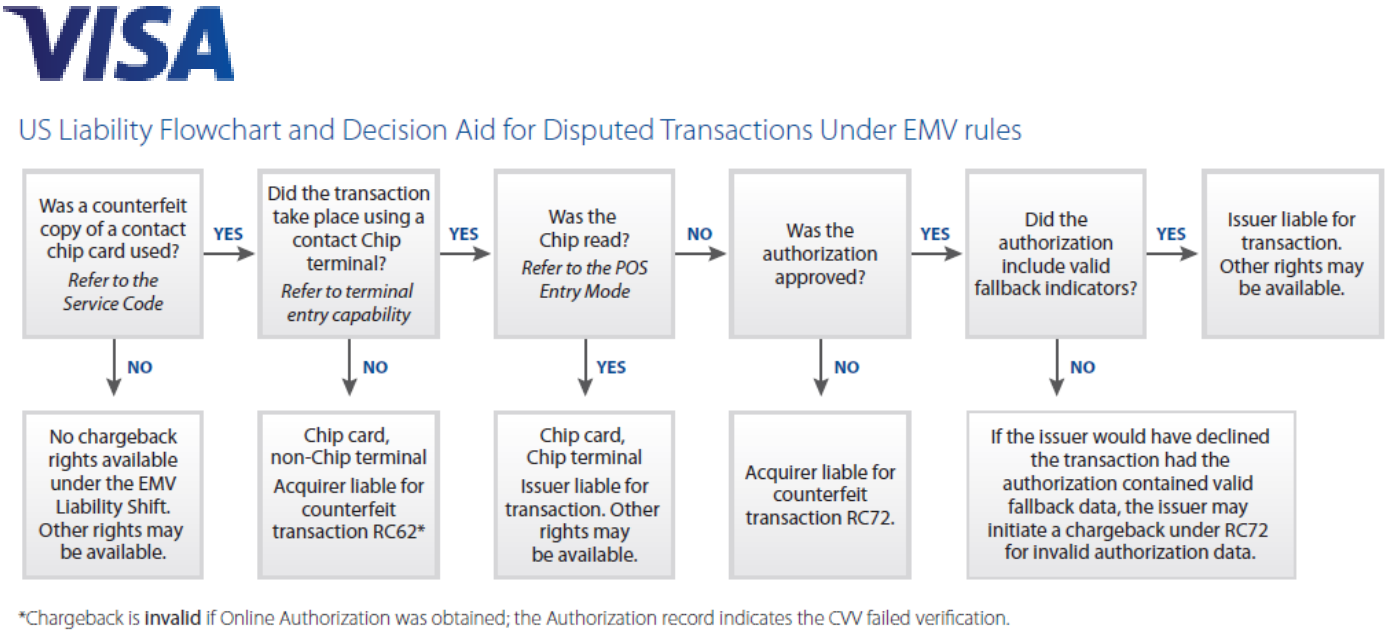
Chip Card (EMV) Chargeback Related Reference



Chargeback rights will only exist under Reason Code 62—Counterfeit Transaction (condition 2) for counterfeit fraud.

Service code of 6 (domestic chip cards) or 2 (first digit – international chip cards)

Terminal entry capability (TEC) of 5 (chip terminal)

POS entry mode code of 05 (chip read) or 95 (chip read)

Chargeback reason codes (MasterCard only):

4870 Counterfeit. EMV service code must be 2XX or 6XX – if a value of 1XX has been authorized then this chargeback code could not be applied as the issuer has authorized a magnetic stripe transaction.

Counterfeit liability shift likely chargeback outcome table

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

4871 Lost/Stolen. Fraud liability shift also applies to lost/stolen if issuer is EMV PIN preferring and merchant is non EMV, is not PIN capable, or PIN entry device does not work.

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

Lost/stolen fraud liability shift - likely chargeback outcome

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.*

Video Resources:

Visa explains to merchants why they don't want to be the weakest link

Visa: 26 second video on the basic chip card transaction