EMV & Fraud
POS Fraud Mitigation Tips for Merchants
EMV Information

• Merchants may see an increase in Card-Not-Present Fraud as a result of the new EMV standards.
  – Help protect your business from fraud risk by enrolling in 3D Secure programs today!

• The EMV liability shift will supersede the No Signature Required programs.

• Merchants should continue to utilize their existing reporting tools to monitor EMV chargebacks.
  – Disputes Operations will be systemically checking the validity of incoming Chip/EMV disputes.
  – Note: Visa RC 62 & 81 are shared reason codes therefore disputes will not be separated for EMV liability shift in reporting and you should expect to see increase in these reason codes.

• A fallback transaction occurs when the card was dipped but the chip could not be read therefore the card was magnetically swiped or manually keyed.
  – Visa has a Fallback monitoring program – when an acquiring bank shows fallback at greater than 2.5% of all chip cards presented, the acquirer can be subjected to fines.
  – MasterCard has not implemented a formal Fallback monitoring program.
  – Visa and MasterCard interchange is not impacted in the US for Fallback transactions.
Fraud Chargeback Reason Code

Description:

- Transactions that the cardholder or authorized user claim are unauthorized; the account number is no longer in use or is fictitious, or the merchant was identified as “High Risk” due to excessive fraud.

- * Designates EMV related reason code

<table>
<thead>
<tr>
<th>Reason codes and description</th>
<th>Reason codes and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>57 – Fraudulent multiple transactions</td>
<td>37 – No cardholder authorization</td>
</tr>
<tr>
<td>62 – Counterfeit transaction*</td>
<td>40 – Fraudulent processing of transactions</td>
</tr>
<tr>
<td>81 – Fraudulent transaction – Card-present environment</td>
<td>49 – Questionable merchant activity</td>
</tr>
<tr>
<td>83 – Fraudulent transaction – Card-not-present environment</td>
<td>63 – Cardholder does not recognize potential fraud</td>
</tr>
<tr>
<td>93 – Risk identification service – International only</td>
<td>70 – Chip Liability Shift*</td>
</tr>
<tr>
<td></td>
<td>71 – Chip/PIN Liability Shift*</td>
</tr>
</tbody>
</table>
How to Avoid and Defend Fraud Chargebacks

How to Avoid

• Dip a chip card whenever possible.

• If chip fails, magnetically swipe the card

• If magnetic swipe fails, imprint the card using a valid device.\(^1\) **Ensure imprint is legible. – NO pencil rubbings**

• Do not imprint on the back of the receipt or on blank sales receipts.

• Ensure merchant descriptor matches the name of the business and is displayed correctly on cardholder statements.

• Implement point-of-sale and internal fraud prevention policies such as checking for ID, comparing signatures on the card to the draft, entering the last 4 digits of the card into the POS, and performing AVS when possible.

• Retain permitted consumer data for research purposes or to allow contact when applicable.

• Utilize alternative account verification sources (e.g. negative databases, fraud screening tools, account updater, or other means to validate the cardholder’s identity).

How to Defend

• Provide a signed, imprinted or magnetic swiped copy of the transaction document.

• Provide a written letter of acceptance from the cardholder.

• Follow other instructions provided on the Chargeback Notice.

• Respond with documentation showing a positive Verified by Visa or MasterCard SecureCode response.

• If this information is not available, you may have to work directly with the cardholder to resolve the dispute.

• Provide compelling evidence to support charge. (Not true remedy)

Note: reason codes 75, 81, 83 and MasterCard reason code 37 are invalid if the transaction was electronically captured at the point of sale (swiped, chip, or contactless)
What you need to know about Compelling Evidence

Compelling evidence is documentation provided by the merchant that, while not being a remedy to the chargeback, provides information that supports the merchant’s claim that the transaction was made by the cardholder. Primarily for card-not-present transactions, Visa and MasterCard allow for certain documentation to be used in support of a dispute for fraud, such as the following:

Card-present merchants should provide:

- Sales draft showing the cardholder’s name that matches cardholder letter of dispute
- Additional transactions connected with the disputed transaction, such as upgrades, ancillary charges with a signed receipt and previous transactions that were related, but not disputed
- Documentation (if applicable) showing cardholder’s name, address and phone number, which can be tied to cardholder letter
- Updated pre-arbitration conditions and certification requirements to require issuers to certify that they have contacted the cardholder and addressed the compelling evidence provided during re-presentment. When compelling evidence is provided, issuers are now required to both:
  - Certify that they have contacted the cardholder to review the compelling evidence.
  - Provide an explanation of why the cardholder continues to dispute the transaction.
## Visa EMV Reason Codes

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Valid Dispute for EMV Liability Shift</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| 62          | • Condition 2<br>  
  • Transaction was completed with a Counterfeit Card in a Card-Present Environment<br>  
  • Cardholder denies authorizing or participating in the transaction<br>  
  • Card is a Chip Card<br>  
  • Transaction did not take place at a Chip-Reading Device | • Invalid<br>  
  • Transaction was a Chip initiated Transaction<br>  
  • The Transaction was a Fallback Transaction<br>  
  • With a Fallback EMV Liability cannot be invoked<br>  
  • Merchant has attempted to read mag-strip prior to hand keyed transaction<br>  
  • Merchant had the highest or same security as Issuer<br>  
  • EMV Device |
| 81 (International only) | • Condition 3<br>  
  • Transaction was completed in a card-present environment<br>  
  • The cardholder did not authorize or participate in the Transaction<br>  
  • Card is a PIN-Preferring Chip Card<br>  
  • One of the following:<br>  
    • Transaction did not take place at a Chip-reading Device<br>  
    • Chip-initiated transaction took place at a Chip-Reading Device that was not EMV PIN-compliant<br>  
    • US Domestic Only – Chip – initiated without online PIN and, if the transaction was authorized Online, the Acquirer did not transmit the full-Chip Data to Visa in the Authorization Request | • Invalid<br>  
  • Emergency Cash Disbursement Transaction<br>  
  • Proximity Payment Transaction (Contactless)<br>  
  • Legible Imprint and PIN<br>  
  • Properly processed EMV transaction<br>  
  • Merchant has the highest or same security as Issuer<br>  
  • EMV Device with PIN capability<br>  
  • Transaction was reported as counterfeit Fraud Type 4<br>  
  • Chip Transaction at an unattended terminal approved online |
### MasterCard EMV Reason Codes

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Valid Dispute for EMV Liability Shift</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| 70          | • This dispute can be used if the following apply  
• Cardholder states they did not authorize the transaction  
• Issuer and acquirer are participating Chip Regions  
• Fraudulent transaction resulted from the use of a counterfeit card at a terminal that is not equipped to accept Chip cards and the card was an EMV chip card  
• Voided Cards  
  − Transaction was identified as a face-to-face transaction  
  − Issuer certifies in writing that the unexpired account number identified was not outstanding on the transaction date because all physical cards were recovered, destroyed, or both | • Invalid  
• Mail Order, Phone Order, e-commerce or recurring payment transaction  
• Properly identified contactless transaction  
• Digital Secure Remote payment Transaction or any subsequent transaction related to a partial shipment or recurring payment occurred  
• Authorized Approval received after the Fraud Notification Service Date (FNS Date)  
• Fallback Transaction – Chip attempted, however transaction was key entered or magnetic swipe read  
  • Merchant has attempted to read mag-strip prior to hand keyed transaction  
• Card is not a Chip Card |
| 71          | • Cardholder states they did not authorize the transaction  
• Issuer and acquirer are participating Chip Regions  
• Fraudulent transaction resulted from the use of a PIN-preferring card at a magnetic stripe-reading-only terminal or at a terminal not equipped with a PIN pad capable of checking the PIN offline or where the PIN pad is not present or not working | • Mail Order, Phone Order, e-commerce or recurring payment transaction  
• Properly identified contactless transaction  
• Digital Secure Remote payment Transaction or any subsequent transaction related to a partial shipment or recurring payment occurred  
• Authorized Approval received after the Fraud Notification Service Date (FNS Date)  
• Valid EMV chip/PIN transaction  
• Fallback Transaction – Chip attempted, however transaction was key entered or magnetic swipe  
  • Merchant has attempted to read mag-strip prior to hand keyed transaction  
• Card was not a Chip Card  
• Commercial Payments Account (MAP) transaction |
# Discover EMV Reason Codes

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Valid Dispute for EMV Liability Shift</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| UA05        | • Issuers are not permitted to initiate a dispute for UA05 when the merchant has invested in the Chip technology | • Fallback Transaction – Chip attempted, however transaction was magnetic swiped or hand keyed  
• Card is not a Chip Card |
| UA06        | • Issuers are not permitted to initiate a dispute for UA06 for non PIN – preferring Chip card | • Valid EMV chip/PIN transaction  
• Fallback Transaction – Chip attempted, however transaction was magnetic swiped or hand keyed  
• Card was not a Chip Card |

# American Express EMV Reason Codes

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Valid Dispute for EMV Liability Shift</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| F30         | • Issuers are not permitted to initiate a dispute for F30 when the merchant has invested in the Chip technology | • Fallback Transaction – Chip attempted, however transaction was magnetic swiped or hand keyed  
• Card is not a Chip Card |
| F31         | • Issuers are not permitted to initiate a dispute for F31 for non PIN – preferring Chip card | • Valid EMV chip/PIN transaction  
• Fallback Transaction – Chip attempted, however transaction was magnetic swiped or hand keyed  
• Card was not a Chip Card |