Systems & Operations | Chip 18 February 2016

Best Practices for Processing Chargebacks Related to the EMV Liability Shift

U.S. | *Acquirers, Issuers, Processors, Merchants*

Overview: To help ensure accurate and efficient chargeback processing, Visa outlines some best practices and reminders.

To encourage greater chip card issuance and acceptance, Visa instituted a liability shift in the U.S. for both domestic and international counterfeit point-of-sale (POS) transactions,[1] which took effect 1 October 2015.

To help ensure accurate and efficient chargeback processing, Visa is outlining some best practices and reminders.

[1] Excluding automated fuel dispenser (AFD) and ATM transactions until 1 October 2017.

Clarification of Transactions Ineligible for EMV Liability Shift Chargebacks

Issuers must not charge back counterfeit transactions under Reason Code 62—Counterfeit Transactions, Condition 2, that have a Central Processing Date (CPD) **before** 1 October 2015 in the original transaction record (ID#: 0025017).

AFD and ATM Transactions

Issuers must not initiate chargebacks under Reason Code 62, Condition 2, for U.S. AFD or ATM counterfeit transactions with a CPD before 1 October 2017. Equally, U.S. issuers must not initiate chargebacks for any AFD or ATM transactions outside the U.S. until 1 October 2017.

Other Ineligible Transactions Under Reason Code 62, Condition 2

Issuers must not initiate a chargeback for magnetic-stripe (POS Entry Mode value of 90 or 02) transactions on non-chip enabled cards. To avoid this, issuers can identify their chip cards using the Service Code field with a first byte value of 2 or 6.

Issuers are only permitted to charge back counterfeit fraud using Reason Code 62, Condition 2; lost or stolen, account takeover, and other fraud types are not eligible.

Contactless Tokenized Transactions

Issuers must not initiate a chargeback under Reason Code 62, Condition 2, for tokenized transactions (e.g., ApplePay), originating from mobile payment devices that have been fraudulently provisioned, as they are considered account takeover fraud.

Issuers are also reminded that:

- When initiating a chargeback for tokenized transactions using other reason codes, the issuer must include the primary account number (PAN) and token data.
- Acquirers may represent tokenized transactions if they do not receive the token data in the chargeback.

If a case is sent to Visa for arbitration, Visa will assess filing and ruling fees of $500 per case against the losing party (i.e., against the party that submits a chargeback without the required token data or for a transaction that does not yet qualify for that specific chargeback right).

Other Contactless Transactions

Correctly processed transactions from contact chip-enabled terminals (Terminal Entry Capability [TEC] 5) are ineligible for chargebacks under the U.S. EMV liability shift rules for counterfeit fraud. If the transaction is completed at a contact chip-enabled terminal, regardless of how the card data is captured (i.e., key entry, magnetic stripe, contact chip or contactless chip), the transaction is protected from chargebacks using Reason Code 62, Condition 2, if full chip data was passed in the authorization message for any chip transactions.

Differing TEC Values

Visa has observed scenarios where the authorization record contains a TEC value indicating that the terminal is not contact-chip capable (TEC 2 or 8), but the subsequent settlement record for the same transaction contains a TEC value of 5, which claims that the terminal is contact chip-capable. This violates the Visa Rules, which state:

> An Acquirer must ensure that all Authorization Requests and Clearing Records contain complete, accurate, and valid data. If an Authorization is obtained, any data in the subsequent Clearing Record must be the same as, or consistent with, comparable data in the Authorization Request and Authorization Response (ID#: 0008752).

Violations of this type are serious and may subject clients to non-compliance assessments and the loss of chargeback protection. Visa has established a task force to monitor, track and communicate with affected parties to resolve these cases.

Chargeback and Fraud Reporting Data Quality

Chargebacks initiated under Reason Code 62, Condition Code 2, are only valid for counterfeit POS transactions conducted using a chip card (ID#: 0008190). Issuers must ensure that they provide the appropriate information for such chargebacks—in the form of any declarations and Member Message Texts—so the acquirer can correctly identify the issuers' use of chargeback Reason Code 62, Condition 2. Additionally, the corresponding fraud report must be accurately identified as Fraud Type 4—Counterfeit, and acquirers have a representment right if the fraud type is inaccurate.

Additional Resources

Visit the Visa Chip (EMV) section at Visa Online for more information.

For More Information

Contact your Visa representative.