

## Mitigating Fraud Risk Through Card Data Verification

AP, Canada, CEMEA, LAC, U.S. | Issuers, Processors

**Executive Summary:** Visa provides issuers with best practices for determining transaction fraud risk before approving or declining a transaction and encourages them to use a combination of transaction attributes to mitigate fraud.

The rise of mobile and cloud-based payments allows Visa cardholders to pay via different devices across multiple interfaces.

As payment transaction types diversify, issuers will find it increasingly important to take a holistic approach to managing risk. Issuers can do this by embedding logic in their authorization hosts to evaluate card verification values (e.g., Card Verification Value [CVV], CVV2, Integrated Circuit Card CVV [iCVV], Dynamic CVV [dCVV], etc.) using the point-of-sale (POS) entry mode and the transaction service code. An overview of these three data elements is provided, along with nine best practices issuers should consider to optimize risk management in their portfolios.

### Related Training Available Through Visa Business School:

- [E-commerce Fraud: Tips and Tools to Manage Your Merchant Fraud Risk](#)

### Transaction Data Elements

- **Card Verification Value Types**

CVV, iCVV and CVV2 may be found on the physical card in the magnetic stripe, in the chip or printed on the back, while dCVV is generated at the time of the transaction. Visa includes these unique, distinct codes in all transactions and requires that all cards, including emergency replacement cards, be encoded with them. Card verification values are based on the account number, expiration date and service code and are calculated by applying a cryptographic algorithm to the encoded account information. Since the card verification value used varies according to the interface through which the transaction was captured (e.g. magnetic stripe, card-not-present, contact chip and contactless), issuers can validate the value to block fraud. Issuers verify card verification values online at the time they authorize a transaction. Incorrect values signal potentially fraudulent transactions.

- **CVV—Magnetic-Stripe Interface:** CVV is the unique three-digit number encoded in Track 1 and the Track 2 Discretionary Data field of the magnetic stripe. It is calculated by applying an algorithm to the encoded account information and verified online at authorization. Issuers should always validate the CVV for magnetic-stripe transactions, even when a PIN is present and verified.
- **CVV2—Card-Absent Environment:** CVV2 is the three-digit number printed on the back of all Visa cards, calculated slightly differently using the same algorithm as the CVV. When merchants submit the CVV2, issuers may check it as part of the authorization request for card-absent transactions (or, in the U.S., when a card cannot be read electronically in face-to-face transactions).
- **dCVV—Magnetic-Stripe Data-based Contactless Interface:** dCVV is an authentication technique for the magnetic-stripe data version of Visa payWave contactless transactions. The dCVV is calculated

using the dynamic contactless chip data and sent in the transaction to the issuer, reducing data compromises and counterfeiting.

- **iCVV—Contact or Contactless Chip Interfaces:** iCVV is a value encoded onto the chip Track 2 equivalent dataset that enables issuers to easily detect and decline counterfeit magnetic-stripe cards created from chip card data. **Note:** The correct iCVV value should only be present in a chip-read transaction. Chip-read transactions should also contain the stronger EMV authentication cryptogram, which should be used for authentication instead of iCVV.

Failure of any of these card verification value types may expose a counterfeit card created from compromised magnetic-stripe or chip data. However, such failures may also signal a problem with a genuine card; issuers should therefore investigate repeated card failures to avoid repeated declines.

Fraudsters may also attempt a brute-force attack on card verification value identification or other authentication values by rapidly submitting consecutive transactions until they receive positive authorization from the issuer. Repeated CVV2 failures, in particular, may indicate fraudulent use of an account number where fraudsters do not physically have the card.

- **POS Entry Mode**

The POS entry mode (Field 22) sent with each transaction provides the issuer with information about how the merchant acquired the transaction data. Since the POS entry mode, in combination with other authorization parameters (e.g., POS condition code), identifies the acceptance channel, POS entry mode verification is essential to identify and prevent fraud. The most common POS entry modes include:

- 01—Manual Key Entry
- 05 or 95—Chip read
- 07—Contactless, using chip data rules
- 02 or 90—Magnetic-stripe read
- 91—Contactless, using magnetic-stripe data rules

- **Service Code**

The service code is a sequence of digits that, taken as a whole, defines various services, differentiates card usage in international or domestic interchange, designates PIN requirements and identifies card restrictions. Service codes apply to **all** Visa products. Typical service code examples include:

- 101—Magnetic-stripe card; international use
- 120—Magnetic-stripe card; international use; PIN is required
- 121—Magnetic-stripe card; international use; online authorization required for all transactions
- 201—EMV chip card; international use
- 221—EMV chip card; international use; online authorization required for all transactions
- 601—National-use EMV chip credit and debit cards

**Note:** Service codes 000 and 999 are **not** valid identifiers of card capability or use, and they are solely used to calculate CVV2 and iCVV. Service codes 000 and 999 must not be encoded on the card magnetic stripe. Issuers should decline transactions with these service codes. Failure to do so may result in fraud losses. Service codes are only used to indicate cardholder verification method (CVM) and authorization preferences during magnetic-stripe transactions. For chip-read transactions, the parameters encoded on the chip will be used for this purpose, and these may not necessarily match the preferences indicated by the service code.

## Using Data Elements to Mitigate Fraud

Issuers should consider card verification values, POS entry mode and service codes together to identify logical conflicts and mitigate counterfeit and card-absent fraud. As a prerequisite, issuers should check that the POS entry mode identifies a supported payment interface and that the service code is valid and matches the one encoded on the card. After reviewing an authorization request, issuers should incorporate the corresponding card verification value result as part of the decision process. Validation of the POS entry mode, the appropriate service code and the corresponding card verification value can automatically identify potential fraud, including:

- **Card-Present Fraud Using Card-Absent Data:** Data stolen from a card-absent transaction should not work on a face-to-face interface, as CVV / iCVV / dCVV validation will fail because the fraudster would not have access to genuine values. Issuers should identify and investigate these discrepancies and decline corresponding transactions once identified as fraudulent.
- **Counterfeiting a Magnetic-Stripe Card Using Contactless Chip Data:** Fraudsters may steal data from a contactless card or a mobile phone and apply it to a magnetic stripe. The magnetic-stripe transaction would have a POS entry mode of 90 (magnetic stripe), indicating that CVV should be checked, which would fail because the fraudster would not have access to the genuine value.
- **Counterfeiting Skimmed Chip Data:** Fraudsters may steal data from a chip card (contact or contactless) and apply it to a magnetic stripe. In this case, the magnetic-stripe transaction would have a POS entry mode of 90 instead of 05 / 95 (contact chip) or 07 / 91 (contactless), and the service code would not match the card type. For example, a service code of 000 or 999 is invalid for a swiped transaction with POS entry mode of 90. Verifying the CVV for a magnetic-stripe transaction will reveal the iCVV stolen from a chip card, and issuers should decline the transaction as suspected fraud.
- **Contactless Fraud Using Compromised Magnetic-Stripe Data:** Fraudsters may counterfeit magnetic-stripe card data onto a payment application stored on a mobile device. When using the contactless interface, the issuer should recognize that this transaction has a POS entry mode of 91 or 07, indicating that they should check either dCVV (for 91) or an EMV Cryptogram (for 07). These should fail, as the fraudster would not have access to the genuine value.

Issuers that do not issue contact chip or contactless-enabled products may not have developed the capability to validate the card verification value types associated with these newer interfaces (i.e., dCVV / iCVV). Visa strongly recommends that issuers decline transactions with POS entry modes irrelevant to the products they have issued (e.g., an issuer that has not issued contactless products should decline transactions with a POS entry mode of 91 or 07).

Issuers that participate in digital wallets should ensure that they are in a position to manage both tokenized and non-tokenized contactless transactions. Issuers that only participate in tokenized wallets may either decline all non-tokenized contactless transactions at their own host or have Visa perform this task on their behalf. Clients should contact their Visa representative for further details.

Validating the card verification value type may sufficiently identify a fraudulent transaction. However, with the introduction of different form factors for use across multiple interfaces, Visa advises issuers to use additional data

elements in authorization decisions. Issuers have card verification value processing options that allow Visa to validate on the issuer's behalf.

VisaNet has edits in place that search for invalid service codes, POS entry modes and card verification value combinations, and it will decline the transaction and send decline advice to the issuer / processor. However, Visa encourages issuers to validate card verification values on their own and perform these same checks on all authorization requests.

### Issuer Best Practices

Given the issuer capabilities and data elements available, Visa recommends the following best practices to optimize portfolio fraud management:

- **Prioritize Chip Cryptogram Validation:** For chip transactions, validation of the Application Cryptogram (Cryptogram Version Number 10 or 17) should take precedence over iCVV validation. iCVV validation should only take place if issuers lack chip data for validation, and issuers should still view successful validation as a higher risk transaction.
- **Enable Multi-Part Authorization Review:** When reviewing an authorization request, issuers should incorporate the card verification value result, the service code and the POS entry mode as part of the authorization process. Issuers should check for consistency and alignment among these multiple data elements, including review of chip card authorization requests across POS and ATM transactions, regardless of CVM (e.g., signature, PIN or no CVM).
- **Decline Invalid Service Codes:** Issuers should decline transactions with invalid service codes, such as 999 or 000.
- **Configure VisaNet for Failed Scenarios:** Issuers should review all failed card verification value (CVV, CVV2, iCVV, dCVV) transactions at the issuer host-level rather than leaving the decision to VisaNet stand-in processing (STIP). Use one of the following CVV processing scenarios:
  - **CVV—Always** to ensure that if the CVV fails in STIP, the transaction will be switched to the issuer, if available.
  - **CVV—All Respond** to ensure that the default response code for invalid CVV transactions is "05" decline.

**Note:** These are VisaNet-specific configurations.

- **Activate 'Soft' Block:** Issuers should consider a soft block on accounts where transactions are approved with invalid card verification value until they confirm account activity with the cardholder. This will lower the number of declines on genuine transactions and reduce customer service issues.
- **Decline Questionable ATM Transactions:** Issuers should consider declining cards with invalid card verification values when the transaction originates from an ATM since invalid card verification values are rarely seen in ATM transactions. It is immaterial that PIN verification may have been successful in this scenario; the issuer should not rely solely on PIN verification.
- **Use CVV2 in Risk Protection:** In addition to using CVV2 to authenticate cards in the card-absent environment, issuers should consider using the number to enhance risk protection in other authentication functions, such as verifying cardholder address changes requested by telephone or verifying new card activations.

- **Enact Velocity Rules:** These rules help identify and stop a brute-force attack or testing / probing attacks (when a fraudster may rapidly submit multiple successive low-value transactions) until the issuer gives authorization to obtain a valid card verification value for a specific card. Once the fraudsters obtain an authorization, they will typically conduct higher-value fraudulent transactions immediately until the issuer detects the suspicious activity.
- **Leverage Application Transaction Counter (ATC) Check for Chip Transactions:** Issuers should monitor and track the ATC for chip cards to identify replay attacks by fraudsters. For example, a repeat use of the same ATC for a transaction may indicate such an attack.

Issuers that use proven fraud prevention tools and multiple data elements from authorization requests will be better prepared to mitigate fraud across their portfolios.

### Additional Resources


Valid values for POS entry mode can be found in the *BASE I Technical Specifications, Volume 1—V.I.P. System*.

For a full description of service code values, refer to Section A.5—Data Element Descriptions in the *Payment Technology Standards Manual*.

### For More Information

Contact your Visa representative or email [InfoRisk@visa.com](mailto:InfoRisk@visa.com) with "Card Data Validation" in the subject line.

---

Notice: This Visa communication is furnished to you solely in your capacity as a customer of Visa Inc. (or its authorized agent) or a participant in the Visa payments system. By accepting this Visa communication, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Rules, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or a participant in the Visa payments system. You may disseminate this Information to a merchant participating in the Visa payments system if: (i) you serve the role of "acquirer" within the Visa payments system; (ii) you have a direct relationship with such merchant which includes an obligation to keep Information confidential; and (iii) the Information is designated as "affects merchants" demonstrated by display of the storefront icon  on the communication. A merchant receiving such Information must maintain the confidentiality of such Information and disseminate and use it on a "need to know" basis and only in their capacity as a participant in the Visa payments system. Except as otherwise provided, the Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system.

Please be advised that the Information may constitute material nonpublic information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material nonpublic information would constitute a violation of applicable U.S. federal securities laws. This information may change from time to time. Please contact your Visa representative to verify current information. Visa is not responsible for errors in this publication.