Mitigating Fraud Risk Through Card Data Verification

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

With a number of cardholder payment options (e.g., magnetic stripe, contact chip and contactless chip) and methods in development (e.g., mobile and cloud-based), it is increasingly important for issuers to take a holistic approach across the different form factors and interfaces through which a Visa payment can be made in order to manage the risk associated with each type of transaction.

To help mitigate fraud, issuers should adopt the following tools and data elements to determine the level of fraud risk associated with a transaction before an approve or decline decision is made. Additionally, Visa encourages issuers to consider the combination of transaction attributes when implementing fraud mitigation measures. These tools and data elements are applicable to all form factors and across multiple interfaces, utilizing authorization solutions that offer real-time and stand-in support.

Card Verification Data

Fraudsters target issuers that neglect to validate Card Verification Value (CVV)—a unique and distinct code that verifies that a card is in the possession of the cardholder—in conjunction with other authentication factors to prevent counterfeit, primary account number (PAN) key-entered and card-not-present fraud. As such, issuer validation of the CVV and understanding of the significance of other data elements present in an authorization message during a transaction is key to controlling fraud losses both in the card-present and card-not-present environments.

The CVV can be used to detect a counterfeit card in cases where a magnetic stripe has been encoded or re-encoded with valid account information from other sources. Visa requires that all cards—including emergency replacement cards—are encoded with the CVV, which is calculated by applying a cryptographic algorithm to the encoded account information (card account number, expiration date and service code).

In addition, to prevent fraud from occurring, variations of CVV exist across the different interfaces of Visa transactions:

- **Magnetic-Stripe Interface—CVV:** A unique three-digit code encoded in Track 1 and the Discretionary Data field in Track 2 of the magnetic stripe or the chip magnetic-stripe image (MSI). CVV should always be validated for magnetic-stripe transactions, even if the PIN is present and verified.

- **Card-Not-Present Interface—CVV2:** A fraud prevention technique used in the card-not-present environment to ensure the card is valid. The CVV2 is a three-digit value printed on the back of all Visa cards which can be submitted by the merchant as part of the authorization request. The CVV2 is different than the CVV contained on the magnetic stripe and is validated using a different calculation. CVV2 failures may indicate fraudulent use of an account number where the fraudster does not have the card in hand, and as a result, does not know the CVV2 value.
- **Contactless Interface—Dynamic Card Verification Value (dCVV):** An authentication technique on the magnetic-stripe data version of Visa payWave contactless transactions used to reduce the threat of data compromises and counterfeiting.

- **Chip Interface—Integrated Card Verification Value (iCVV):** A tool used to protect against data being copied from a chip card and applied to the magnetic stripe of a counterfeited plastic card.

- **Chip Cryptogram:** A cryptogram included in the authorization message of chip-based transactions using chip data. The cryptogram should be verified to ensure authenticity of the chip card.

CVV failures during authentication may indicate a counterfeit card was created from compromised magnetic-stripe or chip data. They may also signal a problem with the card itself; repeated failures on a card should be investigated to avoid repeated declines for a cardholder in good standing. Fraudsters may also attempt to identify a CVV or other authentication value through brute force by rapidly submitting consecutive transactions until they get a positive authorization from the issuer.

**Point-of-Sale Entry Mode**

The point-of-sale (POS) entry mode (Field 22)—sent in each Visa transaction—tells the issuer how the transaction data was acquired at the merchant. Because the POS entry mode identifies the acceptance channel in combination with other authorization parameters (e.g., the POS condition code), verification of this information is an essential step to identifying and preventing fraud.

The most common POS entry modes include:

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

**Service Code**

The service code is a sequence of digits that—taken as a whole—allows the issuer to define various services, differentiates card usage in international or domestic interchange, designates PIN and authorization requirements and identifies card restrictions. The use of a service code is applicable to all Visa products.

Typical service code examples are:

- 101—International-use credit and debit cards
- 120—International-use credit and debit cards where PIN is required
- 201—EMV chip credit card
- 221—EMV chip debit card
- 601—Domestic-use EMV chip credit and debit cards
Note: Service codes of 000 or 999 are not valid as identifiers of the card capability or usage, but rather are used in the calculation of CVV2 or iCVV. Therefore, service codes of 000 or 999 should not be encoded on a magnetic stripe. Visa is aware of scenarios in which either 000 or 999 has been encoded on the magnetic stripe of counterfeit cards, resulting in issuer fraud losses.

Use of Data Elements to Mitigate Fraud

CVV values, POS entry modes and service codes should be used in combination to identify logical conflicts and mitigate preventable counterfeit and card-not-present fraud. Issuers need to ensure that the POS entry mode identifies a supported payment interface and that the service code is valid. After reviewing an authorization request, issuers must incorporate the corresponding CVV result as part of the decision process. When an issuer validates the POS entry mode, the appropriate service code and the corresponding CVV, they can automatically identify potential fraud, as illustrated in the following examples:

- **Card-present fraud using card-not-present data:** Data stolen from a card-not-present transaction are applied to a face-to-face interface. The expected CVV code on the card-present interface would not match up to the CVV2. Issuers’ validation should identify this discrepancy and decline the transaction.

- **Counterfeiting a magnetic-stripe card:** Data stolen from a mobile phone are applied to a magnetic-stripe interface. The magnetic-stripe transaction would have a POS entry mode of 90 (magnetic stripe) instead of 91 (mobile contactless). Verification of the CVV would reveal that it is incorrect for a magnetic-stripe transaction.

- **Counterfeiting skimmed chip data:** Data stolen from a chip card are applied to a magnetic-stripe interface. The magnetic-stripe transaction would have a POS entry mode of 90 (magnetic stripe) instead of 05 or 95 (chip) and the service code should support the type of card that is being used. A service code of 999, used to calculate the iCVV value, is not valid for a swiped transaction. Verification of the iCVV would reveal that it is incorrect for a magnetic-stripe transaction and the transaction should be declined as suspected fraud.

- **Contactless fraud using compromised magnetic-stripe data:** A fraudster has counterfeited a magnetic-stripe card onto a contactless interface on a mobile device. When using the contactless interface, the bank should first recognize that this transaction has a POS entry mode of 91 or 07 (contactless) instead of 90 (magnetic stripe). The expected CVV for a contactless interface should be dCVV or iCVV.

The validation of CVV itself may be sufficient to deny a fraud transaction. However, with the introduction of different form factors for usage across multiple interfaces, Visa recommends that issuers consider additional data elements in order to appropriately decline fraudulent transactions.

Issuers are provided with multiple CVV processing options, including the option to allow Visa to perform CVV validation on the issuer’s behalf if the issuer has delegated the validation to Visa. VisaNet has edits in place that will look for invalid CVV, POS entry mode and service code combinations, and will decline the transaction and send a decline advice to the issuer / processor. Visa encourages issuers that are validating CVV on their own to perform the same checks on all authorization requests.

Issuers can also setup the Visa Risk Manager Real-Time Decisioning (RTD) system to decline transactions that do not meet their approved criteria (e.g., invalid service code).
Best Practices

1. When reviewing an authorization request, issuers should incorporate the CVV result, POS entry mode and service code as part of the decision process. Regardless of cardholder verification method (CVM), this should include a review of authorization requests on chip cards (i.e., signature, PIN or no CVM).

2. Issuers should decline transactions where the service code is invalid, such as when 999 or 000 is encoded on the magnetic stripe and the attempted POS entry mode is 02, 90 or 91.

3. Issuers should review and authorize all failed CVV transactions at the host level rather than leaving the decision to stand-in processing. Use one of the following CVV-processing scenarios:
   - **Always:** To ensure that if the CVV fails in stand-in processing, the transaction will be switched to issuer processing, if available.
   - **All Respond:** To ensure that the default response code for invalid CVV transactions is 05 decline.

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

4. After identifying an approved transaction with an invalid CVV, issuers should consider a "soft" block until the account activity has been confirmed with the cardholder. This will reduce the fraud transaction count in the event that the transaction is denied, and will in turn lessen the fraud amount loss per account.

5. Issuers should consider using a decline response for a card that has an invalid CVV when the transaction originates at an ATM, as invalid CVVs are rarely seen on ATM transactions. It is irrelevant if PIN verification may have been successful in this scenario.

6. In addition to using CVV2 as a card authentication tool, issuers should consider using it to enhance fraud protection in other situations, such as verifying cardholder address changes (requested by phone) or new card activations.

7. Issuers should enact velocity rules to identify and stop brute-force, testing or probing attacks, where fraudsters may rapidly submit multiple successive low-value transactions until they get a positive authorization from the issuer. Typically, once the fraudsters obtain an authorization they will immediately conduct higher-value fraudulent payments until the issuer detects the suspicious activity.

Clients that use proven fraud-prevention tools and make use of multiple data elements that are present in authorization requests will be better prepared to mitigate fraud across their portfolio, regardless of the form factor or interface.

**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 digit values, refer to Section A.5, Data Elements Descriptions of the *Payment Technology Standards Manual*. 
For more information or for clarification related to the validation of CVV, POS entry mode and/or service code, contact your Visa representative or email 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 Visa’s operating regulations, 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. 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. The Visa Non-Disclosure Agreement can be obtained from your Visa Account Manager or the nearest Visa Office.