



Risk Management & Fraud Detection Services

Visa Debit Processing Service

Overview

Visa® Debit Processing Service offers a variety of flexible risk management services to help your financial institution reduce losses and lower administrative expense associated with managing fraud. Our comprehensive risk management services range from suspect activity reporting to advanced neural network fraud detection support.

Visa Debit Processing Service works closely with you to identify your risk management needs and then provides tools and controls to actively manage payment system risk. You may take advantage of any or all of the options available and, as your risk management needs change, easily adjust program parameters.

Your single-point connection to Visa Debit Processing Service helps you make informed authorization decisions to manage risk, while also achieving your customer service objectives.¹

Benefits of Risk Management & Fraud Detection Services

- **Protect your card programs with comprehensive fraud management coverage.** Visa tailors services to your financial institution's needs, risk characteristics, and goals. By combining processing scale, advanced technology, and years of risk management experience, we can provide you with a complete fraud management program at an affordable cost.
- **Reduce fraud losses.** Visa employs advanced fraud detection tools—including Falcon™ Fraud Manager,² Visa Advanced Authorization, and Flash Fraud Rules—to protect your Visa card programs from intrusion by unauthorized users and to combat flash fraud.
- **Improve authorization decisions.** Information supplied by Visa Advanced Authorization and other authorization parameters enhances your authorization decision-making process, bringing security and increased confidence to each Visa payment card authorization.
- **Protect cardholders with world-class customer service.** You can depend on Visa Cardholder Support Services (CSS) for full-function fraud call center services including monitoring, rules management, confirmation calls, high score/non-contact block options, and 24/7 voice response unit (VRU) access for cardholders to block/unblock and activate their cards.
- **Reduce costs and minimize resource requirements.** When you choose CSS for fraud call center support, all equipment, systems, and personnel reside at Visa, reducing your costs and minimizing the resources required for full-function fraud detection protection.

Key Features

Fraud Detection Services

- **Neural network technology.** Visa operates Fair Isaac's Falcon Fraud Manager, a neural network platform that performs sophisticated fraud scoring to capture relationships and patterns often missed by traditional fraud detection methods. This advanced system enables you to design customized anti-fraud strategies to successfully detect and stop potentially fraudulent activity. The system also provides operational and statistical reports to help you measure the success of your anti-fraud program.

Primary system components include:

- **Falcon Debit™.** In conjunction with the Visa authorization system, the Falcon Debit scoring engine uses neural network-based statistical models and computational techniques to calculate a fraud score for each transaction based on individual cardholder and transaction data. If the score indicates a high probability of fraud, the system can create a fraud case and send it to a fraud analyst for action, block subsequent transaction attempts, or both. The fraud score also may be used to make real-time authorization decisions.

Key Features (continued)

- **Falcon Expert™.** Falcon Expert provides the ability to define rules to automate fraud prevention procedures. This rules-based capability allows the use of other relevant transaction data fields, in addition to the fraud score, when determining fraud actions.
- **Flash Fraud Rules.** Flash Fraud Rules provide a parameter-driven set of rules to help catch and block suspect transactions falling into specific risk categories. Flash Fraud Rules are temporary rules to catch isolated fraud and stop authorization requests prior to approval. They may be used alone or in conjunction with Falcon.

The following fields may be used to block fraudulent transactions:

- Merchant country code
- Merchant category code
- Merchant ZIP code
- Acquiring network ID
- PAN entry mode
- Transaction amount range
- CVV checked indicator
- CVV result
- BIN
- Prior Falcon score
- Visa Advanced Authorization Risk Score or Risk Condition Code
- Visa CAMS alert ID

Call Center Services

- **Fraud call center services.** Visa Cardholder Support Services (CSS) offers a high quality, turnkey fraud call center solution for financial institutions using Falcon Fraud Manager. At your option, you may use CSS support around the clock (full-service plan) or part-time (shared-service plan). Whichever option you choose, Visa fraud analysts monitor your fraud scores, notify cardholders of suspicious activity, and respond to cardholders' inquiries related to their fraud situations.

Fraud call center services include:

- Monitoring Falcon and managing Falcon Expert rules
 - Initiating transaction confirmation calls to cardholders
 - Responding to inbound cardholder calls on a dedicated toll-free number unique to your financial institution
 - Blocking accounts on high-risk cases or in confirmed fraud situations
 - Communicating blocks and confirmed fraud conditions
- **Hot card/card activation services.** In addition, CSS supports hot card statusing and card activation services. CSS can accept lost/stolen card notifications and card activation requests 24/7 from your cardholders. Around-the-clock hot carding helps protect your cardholders and financial institution from potential fraudulent activity. Full-time VRU capabilities enable cardholders to activate their new or reissued cards whenever it's most convenient for them.

Authorization Services

- **Authorization edit checks.** Risk edits and authorization processing options help reduce your fraud exposure. Edit checks may be set at the financial institution, card group, or individual cardholder level. You may set limits separately for cash and POS activity, and timeframes may be set for single- or multiple-day periods.³ Authorization edit checks include, but are not limited to:
 - **Daily spending limits.** Monitors dollars spent and cash back.
 - **Velocity checks.** Monitors the frequency of card use.

Key Features (continued)

- **Expiration date checks.** Determines if the card is expired and/or checks for an exact expiration date match.
- **Name match.** Reduces the risk of skimmed and counterfeit cards by comparing the Track 1 names on incoming authorizations to names on file. Name match also may be used to create more robust authorization rules in Falcon.
- **PIN validation.** Verifies entered PIN to the PIN value on file (available for ATM and select point-of-sale transactions).
- **Visa Fraud Protection Programs.** For greater card program protection and reduced fraud, these programs validate additional data in the authorization message:
 - **Cardholder Verification Value (CVV).** Validates a unique three-digit code on the magnetic stripe of all cards to detect counterfeit or re-encoded cards.
 - **Cardholder Verification Value 2 (CVV2).** Verifies a unique value, printed on the reverse side of the card, to reduce fraudulent card-not-present transactions.
 - **Dynamic Cardholder Verification Value (dCVV).** Validates a dynamic three-digit code provided by the chip on a contactless card to detect fraud.
 - **Address Verification Service (AVS).** Enables merchants to confirm a cardholder's billing address to prevent fraud in the card-not-present environment.
- **Verified by Visa (VbV).** VbV makes Internet purchases safer by authenticating a cardholder's identity in real time during an online Visa card transaction. Cardholders are asked to enter a password to validate their identity during the authorization process.
- **Visa Advanced Authorization.** Visa Advanced Authorization, an enhancement to the VisaNet authorization message, is a risk evaluation system that provides risk information directly for 100 percent of VisaNet-processed authorizations (initiated with a U.S.-issued Visa card). Robust risk information enables you to make real-time decisions that can potentially stop losses with the first transaction and enhance the security of Visa payment card authorizations. Visa Debit Processing Service has developed fraud rules to stop activity based on Visa Advanced Authorization scores. Risk information is provided in the form of:
 - **Risk Scores.** Uses predictive fraud models to indicate the probability that the authorization is fraudulent.
 - **Risk Condition Codes.** Provides descriptive information for accounts associated with a high-risk compromise event (e.g., a compromised account or an account-generation scheme), as identified across the entire VisaNet payments system and potentially across multiple issuers.Once you receive Visa Advanced Authorization's risk information, you are empowered to take appropriate action based on your authorization risk strategies and parameters and/or send the risk information into downstream risk management systems such as Falcon Fraud Manager.
- **Stand-in processing.** Visa authorizes transactions on behalf of your host system when it is unavailable or when you have chosen Visa to process certain transaction on your behalf. Before authorizing a transaction, Visa reviews your cardholder file, your specified limits, and your transaction data check options to handle the transaction according to your specifications.
- **Suspect activity reporting.** A suite of reports can help identify excessive or abnormal cardholder activity levels. Configurable reports can monitor transaction counts and dollar limits for single- or multiple-day periods.

The Visa Debit Processing Service Advantage

For More Information

- **Customer-focused.** Meeting your payment product and service needs is our business and our priority.
- **Integrated processing solution.** Reach your objectives with the Visa solution for success in the debit and prepaid marketplaces.
- **Continuous access and security.** You're covered with reliable, state-of-the-art processing and security technology.
- **Single-point connectivity.** One connection simplifies your Visa and EFT product processing needs.
- **Proven service.** Specialized client team is dedicated to helping you meet your card program goals.

For more information, please contact your Visa Account Executive or Visa Debit Processing Service at (800) 611-1426 x7673.

¹This document is intended for descriptive purposes only. For more complete information regarding these services, please contact Visa Debit Processing Service.

²Falcon is a registered trademark of Fair Isaac Corporation.

³Edit options available to your financial institution depend on the type of file you provide to Visa Debit Processing Service.

