MAP
MEMBER ACCESS PROCESSING

*Dynamic Payment Solutions. Trusted Results.*

# Risk Management

Member Access Processing offers a variety of flexible risk management services to help your credit union 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.

MAP works closely with you to identify your risk management needs and then provides tools and controls to actively manage payment system risk. An integral part of our comprehensive risk solutions, our advanced fraud management platform analyzes every transaction using sophisticated fraud scoring that protects you and your members.

## Key Features

MAP's Fraud solution takes advantage of three real-time fraud monitoring systems; FICO Falcon Fraud Detection Service (Falcon) using Falcon Fraud Manager Server 6.4, Visa Advanced Authorization (VAA) and Risk Services Manager (RSM). These three systems are integrated and work together with a our managed service models, Managed Real-Time (MRT) or Risk Advisor (RA), to produce average client fraud rates 36% lower than the Visa national average.

**Falcon Fraud Manager.** MAP operates FICO Falcon Fraud Manager, Server 6.4, a neural network platform that performs sophisticated fraud scoring to identify relationships and patterns often missed by traditional fraud detection methods. Use it to design customized anti-fraud strategies that 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. MAP's fraud detection services are available in one of three levels, depending on the needs and capacity of the financial institution:

Full-Service—Visa DPS Call Center staff monitor all suspected fraud cases on MAP's client's behalf on a 7 x 24 x 365 basis.
Shared-Service— MAP's client monitors all cases during regular business hours, with Visa DPS filling in during non-business hours.
Stand-Alone service— MAP's client defines its own case management strategies, and works all of their own suspected fraud cases during the hours that they define.

MAP supports Falcon SMS 2-Way Text Message Alerts and Falcon Interactive Emails to notify cardholders of suspected fraud. The cardholder has the option to respond to the notices via text, email or call center.

**Visa Advanced Authorization (VAA).** VAA is a comprehensive risk management tool that monitors and evaluates VisaNet authorizations in real time, helping you immediately identify and respond to emerging fraud patterns and trends. As transactions are processed through the VisaNet system, VAA evaluates the authorization request data and assesses and assigns risk, allowing you to evaluate and make more informed decisions. Financial institutions that process through MAP may exclusively receive the VAA score on all their transactions, regardless of the acquiring network used by the merchant.

**Risk Services Manager (RSM)** provides an easy-to-use, client-managed rules engine to help catch and block suspect transactions. These rules may be used alone or in conjunction with Falcon Fraud Manager and are especially effective at catching unique fraud incidents, enabling you to stop authorization requests prior to approval.

**Managed Real-Time (MRT).** Our full-service call center clients can further protect their card programs with Managed Real-Time Decisioning, a real-time rule strategy developed by Visa DPS fraud experts based on actual performance and configurable for your business. Rather than simply targeting rules to current fraud patterns and trends, our real-time decisioning solution uses multi-faceted risk intelligence data and actual false positive rate performance to determine the most effective real-time decline strategies to help you reduce fraud.

## Key Features (continued)

**Risk Advisor** is a full-service fraud solution that provides clients consulting services and regular reviews to discuss fraud trends and overall performance including custom-designed monthly reporting and performance insights into benchmarking, authorization, and fraud information across a variety of segments. It includes customized real-time decline ruleset based on client input on risk tolerance and fraud profile and comprehensive monitoring of defined, higher risk transaction segments every day, including weekends and holidays.

**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.

**Hot Card/Card Activation Services** can accept lost/stolen card notifications and card activation requests 24/7 from your cardholders. This around-the-clock support helps protect you and your cardholders from potential fraudulent activity. Full-time VRU capabilities enable cardholders to activate their new or reissued cards whenever it's most convenient for them.

**Issuer Cardholder Authentication Service (ICAS)** uses a Risk-Based Authentication (RBA) method that occurs in real-time without introducing friction into the cardholder's online shopping experience. ICAS can be implemented as a pass/fail, entirely frictionless experience or as a pass/fail/challenge option.

**VIP Travel Monitor Service** allows you to designate individual cardholders for special transaction processing and manual fraud case review. It provides a premium, 24/7 monitoring capability that enables cardholders to verify transactions using a dedicated toll-free number.

**Visa Data Manager** provides state-of-the-art fraud analytics and insights tools, allowing you can identify the common point of purchase, and then establish a potential list of impacted cardholders for immediate, proactive communication.

**Visa Fraud Protection Programs.** For even greater card program protection and reduced fraud, MAP provides complete support for the following Visa fraud detection programs:

> **Address Verification Service (AVS).** Enables merchants to confirm a cardholder's billing address to prevent fraud in the card-not-present environment.
> **CAMS Alert Service** notifies financial institutions of accounts that are at risk due to a compromise event. Issuers can optionally use this information to make informed decisions about their at-risk accounts.
> **Cardholder Authentication. (CVV/CVV2/dCVV Checking).** Visa DPS provides a range of options for verification of card CVV values as part of the suite of authorization controls provided to client issuers.
> **Fraud Report System (FRS)**. Fraud Reporting System is an application that allows Issuers to electronically report all of their fraudulent transaction through VisaNet. It does not allow you to report Regional Network Fraud.
> **Name Match Service** compares the Track 1 names on incoming authorizations to names held on file at Visa. When a name mismatch is found, that information can be used in the authorization decision.
> **Suspect Activity Report** is a daily report customized to your institution's parameters, quickly identifies excessive or abnormal levels ofcardholder authorization activity.
> **Visa Resolve Online (VROL)** can be used to submit fraud advices and exception file listings to Visa.
> **Visa Resolve Online Real-Time (RTSI)** provides Web services (APIs) that allows a financial institution's host system to add, change or delete a fraud advice.
> **Visa Travel Notification Service (VTNS).** Incorporating cardholder self-reported travel plans into the VisaNet authorization message (e.g. via an online form or your call center), VisaNet informs you whether your cardholder is transacting during the travel dates and at the travel destination provided.

## For More Information

Please contact your Member Access Processing Sales Representative, Relationship Manager, or send us an email at sales@MAProcessing.com.