Enterprise Fraud Risk Management

The Fight Against Fraud

New and sophisticated security threats surface daily in this high velocity electronic payments world. They keep pace with the surge in ecommerce activity, cross-border money movement, mobile transactions, real-time payments and innovative payment methods such as biometric and blockchain payments. Online information sharing and multiple access points open up additional opportunities for cybercriminals. EMV enabled POS terminals move fraud from in-store to online. Financial institutions already under the pressure from new regulations and rising customer expectations experience crippling high-profile data breaches damaging their goodwill and reputation.

To survive in this volatile environment, payment companies need an enterprise-wide scalable and flexible fraud detection solution that must stay ahead of criminal activity.

No One Size Fits All

Fraud occurs at various levels for different stakeholders in the payments ecosystem. While transaction fraud has always been a burden for the payment networks, other participants like merchants routinely face fraud at the point of sale, acquirers deal with fraudulent merchants and customers, and issuers must defend against deceitful cardholders. To combat fraud, merchants need solutions for identity checking and EMV, while acquirers, networks and issuers must focus on rule-based data models. Issuers have the additional responsibility of protecting cardholder data.

Fraud risk management solutions must be customized to address the specific vulnerabilities of these payment providers while adhering to regulatory standards, best practices, customer data privacy and data localization laws. Unfortunately, even the most respected global companies have little or no flexibility to tailor their products to meet stakeholder needs. Many find it challenging to apply artificial intelligence and machine learning (AI/ML) techniques to the unstructured and often unlabeled data that organizations generate. Nor can they recommend technology stacks that work with both online and offline components, guaranteeing data security and PCI compliance. Building a cost-optimized distributed processing architecture that works under these constraints is a formidable task even for the best-of-breed suppliers of fraud management solutions.

Enterprise Fraud Risk Management Framework from RS Software

A robust Enterprise Fraud Risk Management (EFRM) framework involves comprehensive risk assessment followed by design and implementation of controls for detecting, preventing and responding to fraud.

Over the last two decades, RS Software has worked with leading global networks, building and supporting their risk management platforms, and managing fraudulent activity through all stages of the payments lifecycle:

- pre-authorization & authorization
- in-flight and post-facto
- real time and rule based decisioning
- case management for disputes
- configuration management
- real-time consumer notifications

RS Software is currently developing an ERFM platform for India's national payment network providing fraud alerts across 18 different payment channels. Having successfully architected and built India's digital payment platform (UPI) and the Bill Payment System (BBPS) designed to serve more than 1 billion people, the EFRM system serves as the third pillar of a well-balanced and secure infrastructure paving the way for digital transformation in the country.

In its holistic approach to EFRM, RS Software utilizes modern statistical analysis such as machine learning, artificial neural networks, deep learning, cognitive learning and other modern techniques to analyze the huge volumes of structured, semi-structured and unstructured data from internal, third party and public sources such as social networks.
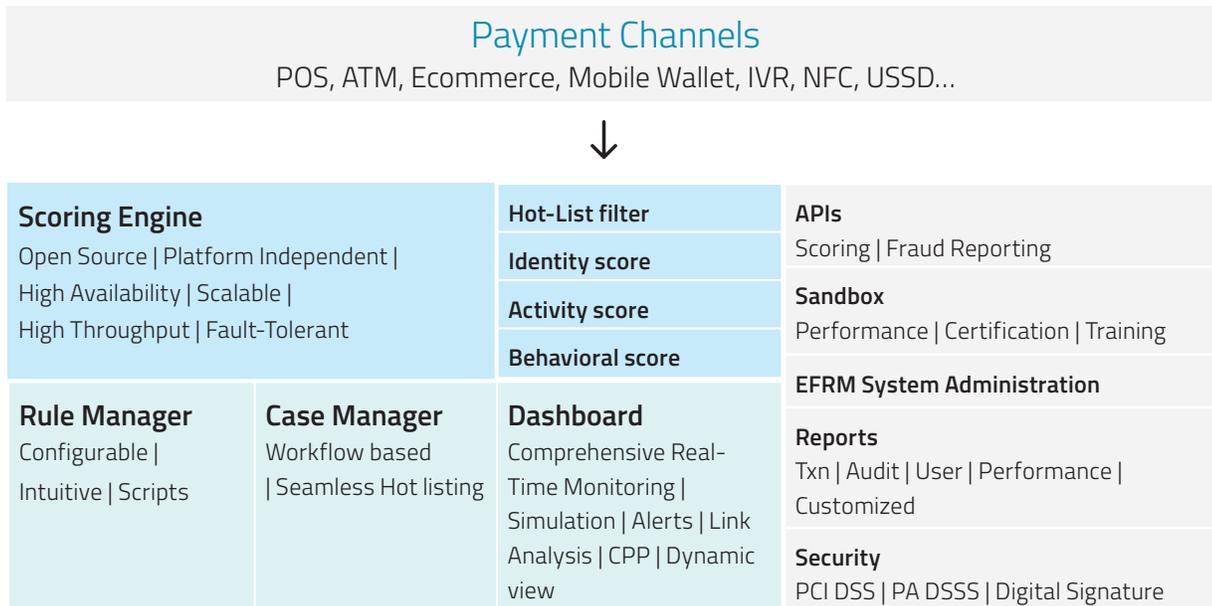
Our EFRM framework can detect and prevent fraudulent activity early in the transaction lifecycle for both online and offline payments across all electronic channels and major payment data formats.

EFRM Framework from RS Software

- Open Source, Best-in-breed, Non-proprietary
- Single solution
  - Across all channels:
    POS, ATM, ecommerce, IVR, cheque, ACH, USSD, Wallet, NFC, Bluetooth, QR Code, Wire, instant payment, P2P, CNP, Payment cards
  - Across major payment data formats:
    ISO 8583, ISO 20022, XML, ISO X.509, JSON, fixed width formats
- Open, Flexible and Dynamic architecture
- Modular and Extensible
- High Availability
- Horizontal and Vertical Scalability
- Parameterized & Configurable
- Platform Independent
- PCI-DSS, PA-DSS Compliant
- High Capacity and Throughput
- Monitoring, Alert & Reports
- Model Accuracy
- Business Continuity Planning

How it Works

The heart of the RS EFRM framework is in its unique Scoring Engine that builds deterministic risk scores from transactions based on Issuing, Acquiring and Network rules. It uses machine learning to continuously monitor, interpret, and update the behavior of each element of every single financial transaction in real time. This leads to a hyperfocused understanding of individual behavior and provides an unprecedented ability to spot even the slightest indication of misconduct. Wherever the data is devoid of any real world context, the Engine employs self-learning AI techniques to detect anomalous payment behavior even while running live in production across P2P payments, wire transfers and other digital transactions.

Payment Channels		
POS, ATM, Ecommerce, Mobile Wallet, IVR, NFC, USSD…		

↓

Scoring Engine Open Source | Platform Independent | High Availability | Scalable | High Throughput | Fault-Tolerant	Hot-List filter	APIs Scoring | Fraud Reporting
	Identity score	Sandbox Performance | Certification | Training
	Activity score	EFRM System Administration
	Behavioral score	
Rule Manager Configurable | Intuitive | Scripts	Case Manager Workflow based | Seamless Hot listing	Dashboard Comprehensive Real-Time Monitoring | Simulation | Alerts | Link Analysis | CPP | Dynamic view	Reports Txn | Audit | User | Performance | Customized
			Security PCI DSS | PA DSSS | Digital Signature

RS Software EFRM Framework - a Component view

The EFRM engine is equipped to handle virtually all types of fraud attacks. The following list is indicative and highlights the more common occurrences:

- **ATM and Debit card Fraud**
  EFRM generates alerts and graphic visualization to pinpoint fraud at its inception before significant losses can occur. It also identifies and isolates the cards at risk to prevent future compromise.

- **Ecommerce Fraud**
  We provide risk based authentication for Card Not Present scenarios taking into account user behavior, devices used, IP address, location and other factors. This facility can be extended to EMVCo QR Code authentication initiated by merchants and cardholders.

- **Instant Payments Fraud**
  Online switch data and offline settlement data from card and bill payments are aggregated to build distinct individual profiles which are stored in-memory to enable superfast rule execution to match the speed of instant payments schemes.

- **Money Laundering**
  Our advanced AML solution accurately monitors customers and transactions for suspicious activity. This includes comprehensive analysis of alerts, decision support systems for invalidating suspicious transactions and electronic filing of Suspicious Activity Reports (SAR) following a suspected incident of money laundering.

Business Value

RS Software's customizable and scalable framework minimizes losses from fraud and maximizes false positives. This is a result of the following core differentiators that gives us an edge over the competition:

- Customizable for merchants, acquirers, issuers, PSPs and others, a feature that is unique across all FRM products available in the marketplace today.

- Built to scale, our framework is flexible enough to scale up as required.

- Near-real-time fraud detection as and when breach occurs is facilitated by a Data Lake built for faster computation and data manipulation.

- Availability across channels & data formats covering all electronic payments channels and all major payment industry data formats.

- Open source technology with no vendor lock-in, reduced hardware cost, simplified license management and easy scaling and consolidation.

- Privacy and security ensured by lack of dependence on customer profiles.

- Rest API based integration makes the solution engine available to third party software.

- Uptime, Speed and Volume designed to handle 2,000 transactions per second with 100-200 millisecond latency.

Why RS Software

RS Software (India) Limited is a global leader in payment technologies. Operating out of US, UK, Singapore and India, we have been in business for more than twenty-five years providing solutions to leading payment brands around the world including payment networks, processors, acquirers, issuers, and banks.

Among our key achievements are mission critical core payment systems for the world's largest card network, transformative digital infrastructure and integrated billing platforms for India, and cutting-edge solutions supporting new payment standards and technologies such as EMV, mobile and contactless payments. Using a proven set of processes, methodologies and state of the art security tools, we build on decades of work for leading brands to protect the payment systems that encircle the globe.

Our proprietary methodology is based on the unique dynamics of the payments industry, and our unwavering focus on domain knowledge, emerging technology and continuous innovation helps our clients stay ahead of the competition.