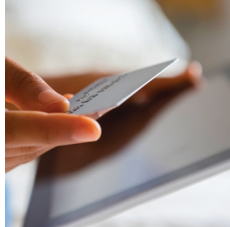


Payment Fraud Manager

Real-Time, Cross Channel Monitoring and Detection for Electronic Payments



Electronic funds transfer fraud presents a global threat to financial institutions, with billions of dollars lost annually. The threat has increased with the shift to faster payments, real-time settlements and the initiation of electronic funds transfers using online and mobile channels.

Since a single, high-value fraudulent electronic funds transfer could compromise a financial institution and even undermine the global financial system, rapid detection of criminal activity is a critical need.

Payment Fraud Manager from Fiserv monitors electronic payments for fraudulent activity in real time across multiple channels. It is the most comprehensive solution available, using advanced inference techniques to identify and prevent fraudulent transactions.

Payment Fraud Manager monitors batch and bulk payment files and individual electronic funds transfer transactions from any initiation channel, including online payments, across payment and messaging infrastructures such as SWIFT, FEDWIRE, SEPA and ACH. It also detects many different attack vectors including batch file manipulation, cybercrime, account takeover and internal fraud.

The solution deploys analytics and risk-scoring models that enable fraud investigators to prioritize highest-risk transactions for review. All data needed to process suspicious payments is available at their fingertips, enabling your organization to rapidly adapt risk management strategies as new fraud patterns emerge.

Payment Fraud Manager allows payment operations and fraud departments to:

- Instantly suspend suspicious payments before losses are incurred, using real-time detection and interdiction
- Control every aspect of risk according to your organization's risk tolerance using supporting scenarios, scorecards and case management
- Respond at the speed of fraud with powerful, easy configuration

Risk Scoring Prioritizes Fraud Risk

Using data and historical fraud pattern analysis, each payment is evaluated for its total fraud risk. Advanced inference techniques are used to understand each consumer's normal behavior related to electronic payments – including frequency, velocity, amount, payment initiation channel and other variables. New transactions are then compared to the individual's normal behavior as well as the normal behavior of a comparable peer group.

When a risk tolerance threshold is exceeded, Payment Fraud Manager creates an alert containing a potential risk score and primary reason codes indicating why the transaction was flagged for review. Flagged transactions are queued according to their scores, so highest-risk transactions can be worked first. Risk scores are based on a wide range of related factors, making it easy for analysts to understand and interpret risk.

Risk tolerance thresholds are set by your management. You control the trade-off between mitigating risk and providing a positive customer experience.

Scenario Center	
CSACH04 - Address Change and Unusual Activity on Dormant Account	750 999 <input type="checkbox"/>
CSBILLPAY11 - Digital Banking Fraud	845.04 999 <input type="checkbox"/>
Indicator	Weight
RecentBillPaymentEnrollment	50 <input type="text"/>
RecentNewPayeeAdded	50 <input type="text"/>
RecentPasswordReset	100 <input type="text"/>
RecentUserIDReset	100 <input type="text"/>
Destination'sNewForOriginatingAccount	150 <input type="text"/>
HighRiskCountryDigitalSessions	350 <input type="text"/>
RecentBadIPAddress	400 <input type="text"/>

Scenario Center: The scenario center is where the administrator can configure the scorecard.

Scorecards and Scenarios Improve Risk Decisions

Payment Fraud Manager lets your staff define their own flash fraud scenarios and weighted scorecards to drive decisions such as blocks, holds or alerts to be worked by analysts. Scenarios and scorecards provide greater control by enabling a fraud manager to assign more aggressive fraud tactics to selected products, channels or customers while prioritizing service over risk for lower-risk or higher-value products, channels or customers.

Scenarios evaluate events to determine risk, target the specifics of a new flash fraud scheme or better protect a customer with a previous fraud event on their account. Your fraud department can easily build its own fraud scorecard by creating scenarios, assigning weights and activating the scorecard.

Scorecards are more powerful than rules because each scenario within the scorecard is given a different level of importance. Assigning weights lets your organization determine the influence that one scenario has over another to improve fraud detection and operational efficiency. All scenarios and

scorecards are customer-centric, rather than generic to your customer base, enabling more accurate results.

Scorecards are valuable for quickly identifying evolving fraud schemes while providing quantitative logic for a decline, hold or approve strategy. Fraud managers have the power to control decisions instantly, before an alert is created. For example, they can automatically decline a transaction with a high score, but allow a lower-risk transaction to go through and generate an alert for further investigation.

Alert and Case Management Provide Comprehensive Risk Views

Payment Fraud Manager generates alerts so that transactions can be researched and decisions made by an analyst. If an analyst verifies a fraud event, a message is sent to the originating system to block the transaction and a case is created in the case manager.

All suspected fraud events are investigated through a configurable and repeatable workflow. The fraud manager or administrator designs queues that can be accessed and worked by groups of analysts.

REF_032: STRONG DEVIATIONS IN OUTGOING PAYMENT ACTIVITY FROM ACCOUNT ACC/4018				
Scenario-Results		Originator Activity	Destination Activity	Customer Info
Code	Name	Result	Score	Thresh...
PFMOG004	Strong Deviations in Outgoing Activity	<div style="width: 100%; height: 10px; background-color: red;"></div>	1050	899
Name	Contribution	Score	Value	Weight
PaymentsFrequencyLast3DaysIsUnusual	<div style="width: 80%; height: 10px; background-color: blue;"></div>	400	True	400
DestinationIsNewForFIInLast3Days	<div style="width: 70%; height: 10px; background-color: blue;"></div>	350	True	350
AmountExceedsUpperToleranceForHistory	<div style="width: 60%; height: 10px; background-color: blue;"></div>	300	True	300
RecentlyOpenedOriginatingAccount	<div style="width: 0%; height: 10px; background-color: blue;"></div>	0	False	100

Scenario Results Detail View: Within the Payment Fraud Alert, the user can view which scorecards and risk indicators are driving the alert and score.

The screenshot shows a web interface for a payment fraud alert. At the top left is the Fiserv logo. The main header area includes navigation and user information. The alert itself is titled 'REF_032 - Suspended' and shows a risk score of 910. Below the score, there are bullet points describing the alert: 'Frequency of payments (of all types) in the last 3 days is unusual', 'Amount exceeds the usual variation tolerance for the originating account', and 'Destination account 13319268 296016 is new to the financial institution within the last 3 days'. A central box displays transaction details: 'From: ACC/4018, Sid Howell Online | 07/30/2017 03:35:47', 'Fedwire 2,190.23', and 'To: 13319268 296016, US'. There are 'Confirm Fraud' and 'Release' buttons. On the right, a 'Related Information' sidebar lists account and customer details. At the bottom, a table (reproduced from the first image) shows the scenario results and contributing factors.

The alert informs the investigator that a transaction has been suspended, and why it has been suspended, and provides investigation tools for the user to make an informed decision on releasing the transaction or opening a case.

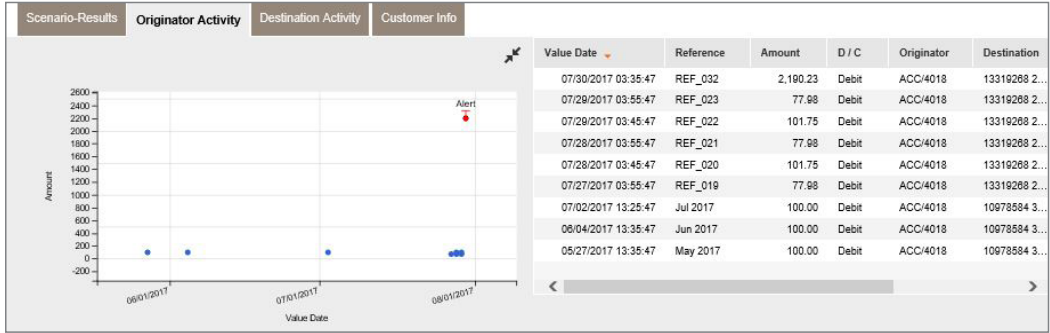
The alert screens provide a comprehensive view of risk. Scores and reason codes indicate the level of risk and indicate where review is recommended. In addition, hyperlinks make it easy to find related information.

Our comprehensive case management system includes:

- Automated data population and investigation workflow
- Transaction, account, customer, channel search and filtering
- Link analysis and graphical network discovery
- Detailed financial data tracking and reporting (risk exposure, preventions and recoveries)
- A digital file cabinet of case information, including any attachments
- Complete audit trails



Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today. Visit fiserv.com to learn more.



Originator Activity Tab: This view of payments sent by the originator gives investigators a clean visual of the current suspended payment and how it compares to historical transactions.



Reporting and dashboards deliver key insights.

Dashboard Reports Deliver Greater Insight

Payment Fraud Manager delivers standard dashboard reports that identify the risk of alerts and transactions in the system. Additional configurable reports can help managers understand and communicate the organization's fraud risk.

Key Benefits

- Instantly suspend suspicious payments before losses are incurred, using real-time detection and interdiction
- Control every aspect of risk according to each organization's risk tolerance using supporting scenarios, scorecards and case management
- Respond at the speed of fraud with powerful, easy configuration

Connect With Us

For more information about Payment Fraud Manager, call 800-872-7882, email getsolutions@fiserv.com or visit www.fiserv.com.



Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
www.fiserv.com