NICE · ACTIMIZE

Payment Gateway Protection

Comprehensive Fraud Coverage at the Payment Rail

Payment Gateway Protection Comprehensive Fraud Coverage at the Payment Rail

The Financial Services world is undergoing a faster payments transformation with new rails and messaging systems emerging across the globe.

Financial Institutions (FIs) will use these new rails to speed up existing payment products and to launch entirely new, innovative faster payment products.

As this transformation takes hold, FIs need fraud controls which are comprehensive enough to cover any emerging rail and which are scalable enough to provide protection for payment product as they are developed.

Actimize Payment Gateway Protection (PGP) provides real-time fraud monitoring for all payments transactions before they leave the banking environment to travel onto payment rails. PGP applies payment-level analytics, which seek out anomalies in transaction patterns and flows without need for channel data. As such, PGP provides comprehensive payment coverage for every rail – complementing channel monitoring, which seeks to discover anomalies in transaction initiation.

In monitoring transactions with payment-level analytics, PGP provides coverage for all off-line or server-to-server transactions, and enables monitoring of relationships between an ecosystem of FIs, corporations, third party senders and individual users.

Key Benefits

- Payment protection scalable enough to handle new schemes and products
- Comprehensive fraud monitoring of outbound and inbound transactions
- Monitoring for “off-line” or server-based payments, including straight-through processing
- Specialized analytics for bank-to-bank transactions
- Analytics tailored to monitor holistic corporate or business payments
  Holistic payment-level monitoring and risk scoring without the need for channel data

Analytics Built to Detect and Prevent Payments Fraud

The Actimize PGP solution applies advanced payment-level analytics which are designed to detect fraud scenarios linked to an array of schemes, such as Real-Time Payments, Wires, ACH, SEPA, Checks, and more.

Central elements of the Actimize PGP analytics approach include:

Expert-Driven Machine Learning Analytics: Actimize fraud detection analytics are trained to recognize a vast array of payment fraud scenarios-- including account takeover, funds abuse, money mule activity, and customer authorized frauds. Models are then continuously enriched by machine learning processes, which discover and incorporate new risk features as fraud threats evolve. Analytics are optimized and expanded to cover new payment products as they are launched.

Behavioral profiles for senders and receivers: Actimize solutions dynamically build entity profiles on both sending and

receiving accounts, which learn “normal” payments behavior and activity, enabling detection of anomalies indicative of fraud. Profiling sending and receiving accounts enables the solutions to detect anomalies to an account or to a wider net of accounts across the financial institution.

Assessing sender-receiver relationship risk: Analytics are configured to assess the transactions of the settlement or firm accounts between the sending and receiving financial institutions to identify suspicious transactions that are potentially modified or inserted during processing. The solution detects corporate account takeovers, insider attacks, or socially engineered customer authorized frauds, to name a few.

“Offline” analytics: Analytics are designed to focus on transactional data without relying on the payment channels where instructions are initiated. Gateway transactions focus on the money-movement that span across many lines of businesses and may contain netted transactions as opposed to individual customer transactions.

Segmented analytics: Segmentation enables fraud monitoring and distinct scoring for monetary transactions based upon their payment or rail type or clearance speeds. For example, analytics apply differing levels of risk based on whether a transaction settles in seconds vs. days.

Holistic view of payment flows: PGP payment analytics focus on money-movement from across all channels and all transaction types related to a monitored account. This unified view of the money-flow detects abnormalities that fraudsters attempt to exploit when fraud systems look at siloed transaction types or channels.

Monitor outbound and inbound transactions: Analytics are designed to evaluate credit and debit transactions which are initiated before going out through the payment gateway as well as to profile those that are received from the payment gateway and are initiated by external financial institutions.

Fraud Monitoring for Outgoing Transactions

The Actimize solution provides specialized coverage for various payment clearing schemes across many lines of businesses, including Real-Time Payments, Wires, ACH, and Checks. Monitor the transactions that your organization send out for clearing.

- Mark, monitor and score outbound transactions
- Supports real-time synchronous fraud risk scoring and interdiction
- Supports on-demand asynchronous fraud risk scoring for batch payments
- Advanced analytics for payment fraud scenarios to help combat account takeover, funds abuse, money mule activity, and customer authorized frauds.
- Analytics provides fraud risk scores on outgoing transactions
- Enables fraud strategies to cancel, delay, or hold funds on outgoing transactions
- Generate alerts
- Capture and store historical transactions for deeper investigation

Fraud Monitoring for Incoming Transactions

The Actimize solution provides coverage for various payment clearing schemes across many lines of businesses, that includes Real-Time Payments, Wires, ACH, and Checks. Monitor the transactions that your organization receives from a payment network.

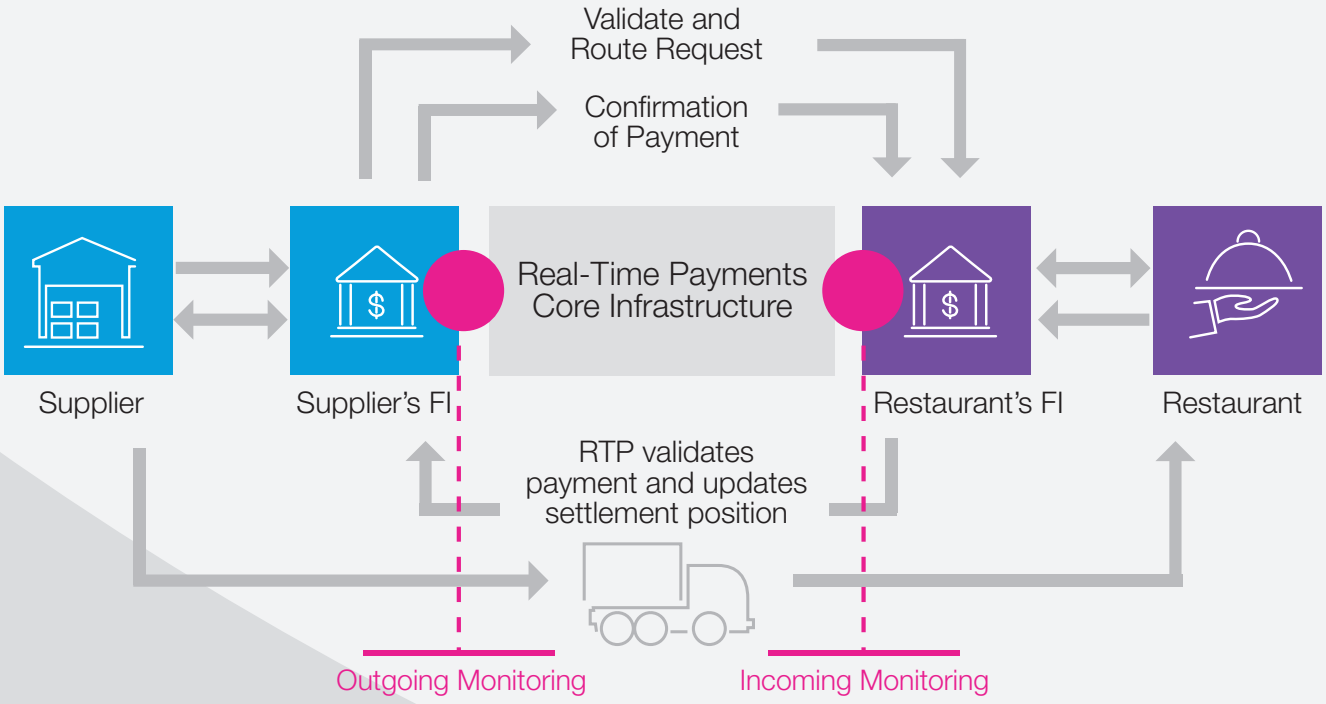
- Monitor incoming transactions
- Supports real-time synchronous processing for incoming transactions
- Supports on-demand asynchronous processing for incoming transactions
- Enable fraud strategies to block transactions, hold funds, or return items, etc.
- Enable fraud strategies that support omni-channel customer experiences
- Generate alerts
- Capture and store historical transactions for deeper investigation

Payment Gateway Protection Use Cases

Business-to-Business Payments: Real-time payment schemes in many markets enable instant payment and settlement between corporations or small businesses with use of messaging systems for invoicing and other communication. With PGP FIs profile entire businesses, holistically monitoring outbound and inbound transactions regardless of payment or transfer product. This unified view of payment patterns detects patterns indicative of corporate account takeover or social engineering earlier.

Business-to-Customer and Customer-to-Business Transactions: New payment schemes enable real-time transactions between corporations and consumers. PGP assesses the risk of relationships between consumers and businesses, and provides monitoring of all outbound and inbound transactions to detect anomalous payment patterns indicative of fraud

Bank-to-Bank Coverage: PGP profiles entire FIs and assesses the risk of relationships between FIs, additionally establishing normal payment patterns between them. As such, PGP provides payment-level analytics, which detect anomalies indicative of fraud in correspondent banking and treasury management.



Payment productsa to emerge.
Gateway needed immediately.

When, Why & How of Payment Gateway Protection

In many scenarios, FIs will employ a combination of channel-centric and gateway-centric fraud monitoring for comprehensive payments coverage.

Actimize applies channel monitoring (Remote Banking and Commercial Banking) to assess the risk of transaction origination using rich channel data, including device identification, geolocation, IP session, authentication history, and much more. With this approach, we protect the channels and specific payment products.

Monitoring at the payment gateway provides a more holistic view of all payments, regardless of channel, traveling in or out of an organization. It serves as a last line of defense for business or corporate users, as well as for third party senders and FIs. PGP assesses the rich data linked to transactions and their messaging systems.

Together, channel and gateway protection provide richer detection across payment products and schemes, catching every suspicious transaction.

Channel and Gateway Monitoring: A Complimentary Approach.

Channel

Why

- Protect the channels
- Find fraud earlier
- Customer experience focus

What

- Originlation requests
- Monetary and Non-monetary
- Authentication

How

- Use channel and auth. data
- Cross-Channel View
- Channel analytics

Gateway

Why

- Total payment view
- Cross-LOB coverage
- Outgoing/Incoming
- Last line of defense

What

- All Payments

How

- Payment analytics
- Anomaly detection
- Catastrophic loss prevention

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.