IBM Counter Fraud Management for Safer Payments

Preventing fraud, in real time, for all payment channels

IBM introduces the industry’s first true cognitive fraud prevention solution to payment processing with IBM® Counter Fraud Management for Safer Payments. Previously marketed as IRIS™ and acquired by IBM in 2016, the solution protects some of the largest and most complex payment portfolios in the world. Payment companies report that IBM Safer Payments significantly reduces fraud losses while keeping false alarms to a minimum. This new approach services all payment channels.

How IBM Safer Payments is different

First generation payment fraud prevention solutions used coded expert experience. This included velocity counters and expert rules to identify high risk. The value of this approach was in its simplicity. However, the ever-increasing number and complexity of fraud patterns have rendered this approach inefficient.

Second generation solutions generated fraud detection models from past data. Neural networks used for this typically require collecting large amounts of data for a long period. This data is then sent to the vendor that creates a model off site. By the time the model is put into production, the fraud patterns it detects can be a few years old.

Next generation IBM Safer Payments’ cognitive approach also uses automatic learning from past data. But rather than generating a black box model, it generates easily readable rules/scenarios. Based on artificial intelligence operating on decades of human experience in its creation of behavior profiles and fraud prevention scenarios, IBM Safer Payments enables a generation of new or revised models with considerably less data and renders faster model update cycles, helping to result in higher fraud detection rates at drastically lower false positive rates.

Highlights

- High fraud detection rates with ultra-low false positives
- Rapid reaction to changing fraud patterns
- Ultra-high throughput with lowest total cost of ownership
Providing value to the payment ecosystem segments

Fraud prevention may be a common goal for all participants of the payment ecosystem, but what this exactly means is not the same for different types of payment companies. IBM Safer Payments has been designed to provide each participant with a solution tailored to their specific needs.

Credit or debit card issuers must keep a tight control on their fraud levels. Though their earnings are small compared to the total transaction amounts, they underwrite the full risk. At the same time, they strive to offer the best customer experience, which is primarily achieved by ensuring legitimate transactions not being declined. IBM Safer Payments is the right solution here because it combines a very high fraud detection rate with ultra-low false positive rates.

For card-present purchases, POS acquirers usually do not bear the fraud losses. However, they must protect themselves against the default risk of merchants and ensure compliance with payment scheme rules. IBM Safer Payments is the right solution here because it combines tight merchant control with the ability to intercept transactions in real time. It also offers specific and configurable reporting on merchant compliance, as well as a complete investigation workflow for merchants violating scheme rules or exposing high-risk behavior.

ATM acquirers operating networks of ATMs have access to a massive number of non-financial messages exchanged on ATM network level, known as “machine events.” IBM Safer Payments is the right solution here because it allows for merging such non-financial transactions to historical profiles and combines these with financial transactions. This enables the detection of ATM channel specific fraud, such as gas attacks, skimmer installation and cash trapping.

E-commerce acquirers facilitate payments for Internet merchants. Because they process card-not-present transactions, their merchants bear the full liability of fraud. IBM Safer Payments is the right solution here because it assesses the individual risk of each merchant. This enables each merchant to accept transactions based on their individual appetite for risk. High-margin merchants typically accept a higher fraud risk with transactions as long as they add to their bottom line. At the same time IBM Safer Payments helps ensure payment scheme compliance.

Figure 1: Real-time analytics monitor the efficacy of the defined profiles, rules and scenarios in preventing the momentary fraud attacks.
Online and mobile banking are attacked by phishing schemes, malware and cybercrime. The challenge is to provide not only fraud security, but also the best possible customer experience. IBM Safer Payments is the right solution here because it profiles the transactions, identifies counterparties and devices, identifies malware—all in the background—with no impact to the customer, nor additional security steps needed. Only when IBM Safer Payments identifies a high risk transaction, will that transaction become the subject of further scrutiny and step-up authentication. This approach also provides compliance with various regulations, such as the revised Payment Services Directive (PSD2) issued by the European Union.

ACH and wire transfers have not traditionally been a prime target for criminals. However, this is changing as these transactions move toward real-time execution. IBM Safer Payments is the right solution here since it allows profiling payment behavior in multiple historical dimensions in real time. Fraud attacks, in which large amounts of money are structured and smurfed through the system using multiple small amount transactions, are securely detected as IBM Safer Payments’ profiling engine restores the true flow of money and securely blocks transactions that are part of such a fraud scheme.

Fintech companies all over the world are working on alternative mobile payment systems that do not rely on card scheme infrastructure. Some are already entrenched in their local economies, while others attempt to disrupt traditional payment practices. IBM Safer Payments is the right solution here because it provides unprecedented flexibility. New data streams can be added in-flight, matched and merged with other data streams, to form a behavioral history that allows for the secure detection of risky and fraudulent activity.

A significant number of IBM Safer Payments’ users are processors or switches that work for multiple banks or other payment providers. IBM Safer Payments is the right solution here because it provides hierarchical multi-tenancy, including inheritance. This enables processors or switches to have generalized models, such as a “region model” or an “industry model,” and allow for each of their tenants to have any kind of bespoke addition to such a model. IBM Safer Payments is PCI PA-DSS certified and designed to be hosted by a payment processor as a service to its processing clients.

For more information
To learn more about IBM Counter Fraud Management for Safer Payments contact your IBM representative or IBM Business Partner, or visit: ibm.com/saferpayments.

Figure 2: Artificial intelligence identifies emerging fraud patterns and automatically suggests new rules/scenarios to prevent fraud losses.