IBM Safer Payments

Preventing fraud, in real time, for all payment channels

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

IBM introduces the industry's first true cognitive fraud prevention solution to payment processing with IBM Safer Payments. This solution protects some of the largest and most complex payment portfolios in the world, significantly reducing fraud losses for financial institutions and payment providers across virtually any payment channel while keeping false alarms to a minimum.

How IBM Safer Payments is different

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

The 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 and 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.

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 the participant's 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 helps achieve this balance of fraud prevention and frictionless experience by providing institutions with a very high fraud detection rate with ultra-low false positive rates.

For card-present purchases, *point-of-sale acquirers* usually don't 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 helps acquires combine 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 the ATM network level, known as “machine events.” IBM Safer Payments provides better fraud detection through greater context by merging non-financial transactions to historical profiles and combines these with financial transactions. This process 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 helps enable each merchant to accept transactions based on the merchant's 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.

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 profiles the transactions, identifies counterparties and devices, identifies malware — all in the background — with no impact to the customer, and no 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.

Why IBM?

IBM Safer Payments puts modern machine learning into the hands of on-site fraud management teams. This enables them to adapt more quickly to changing threats and the introduction of new payment products by dramatically shrinking the time it takes to test and deploy new profiles, rules and models. Using a unique cognitive computing approach, IBM Safer Payments profiles the behavior of any entity and delivers best-fit analytics interactively to fraud professionals. This proven technology is already protecting some of the world's largest and most complex payment portfolios. Outthink fraud by rethinking detection.

About IBM Watson Financial Services

IBM works with organizations across the financial services industry to use IBM Cloud, cognitive, big data, RegTech and blockchain technology to address their business challenges. Watson Financial Services merges the cognitive capabilities of Watson and the regulatory expertise of Promontory Financial Group to help risk and compliance professionals make better informed decisions to manage risk and compliance processes. These processes range from regulatory change management to specific compliance processes, such as anti-money laundering, know your customer, conduct surveillance and stress testing.

For more information

To learn more about IBM Safer Payments, please contact your IBM representative, IBM Business Partner or visit ibm.com/saferpayments.