IBM Safer Payments

Real-time fraud prevention for all cashless payment systems

Highlights

- High fraud detection with false positive rates as low as 1:3
- Open source data science platform for rapid response to new fraud vectors
- Fraud modeling augmented by AI-generated rules
- Ultra-high throughput, 99.999% availability and extremely low latency

IBM Safer Payments, the industry's first true cognitive fraud prevention solution, brings agility to the fraud practice with its open source data science platform. The solution protects some of the largest and most complex payment portfolios in the world across all cashless payment systems, helping card issuers & acquirers, network operators and payment processors optimize for higher fraud detection and lower false positive rates.

How is IBM Safer Payments different?

The first-generation payment fraud prevention approach relied primarily on expert driven rules to identify high risk transactions. The value of that approach was its simplicity. However, the ever-increasing volume and complexity of fraud attacks with the adoption of real time payments have rendered this approach inefficient.

The IBM Safer Payments cognitive approach involves learning from past transactions to generate best-fit rules that fraud analysts can use to optimize existing models or build and deploy new models in minutes, as opposed to weeks. Competitive features of this solution that you can take advantage of allow you to apply machine-learning where it's most effective — in daily payment-channel management. Additional key features follow.

- Build and deploy models whenever needed to address new fraud threats—in minutes.
- Add direct threat detection to conventional detection by deviation from normal.
- Turn widespread, ad hoc rule development into an optimized AI process of rule discovery.
- Process any transaction type and easily share data between types for best detection.
- Make use of fully transparent, user-controlled models, rules, variables, profiles, roles and interfaces.
- Support hundreds of concurrent portfolios and their models for processors and networks.
- Benefit from very fast real-time monitoring and model-building because full history is kept in memory.
- Rest assured with 99.999% availability by triple redundancy on low-cost, x86 Linux equipment.
- Change transaction types, variables, models, UI; even software, while running at full load.
- Achieve high detection at extremely low false-positive rates.

Fight fraud across all cashless payment systems

Fraud prevention may be a common goal for all participants of the payment ecosystem, but its definition varies by participants. IBM Safer Payments is designed to provide each participant with a solution tailored to specific fraud objectives and KPIs.

Current fraud detection technologies fall short of responding to fraud in the era of real-time payments and P2P payments. Banks and payment processors realize the need for a new, more agile way of addressing fraud and threats as they emerge. IBM Safer Payments enables fraud department leverage peer profiling, cross channel profiling, third party open artificial intelligence and machine learning tools, and non-financial data from devices, online interactions, and more to fight fraud in faster payments.

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 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 combining 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. The IBM Safer Payments solution addresses this issue by allowing 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. However IBM Safer Payments is unique 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 delivers powerful capabilities for 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 and model building tools in the hands of on-site fraud management teams so they can respond faster to new fraud vectors without much dependence on vendor and data science teams. Using a unique cognitive computing approach, IBM Safer Payments profiles the behavior of customer segments and delivers best-fit analytics interactively to fraud professionals. This technology is already protecting some of the world's largest and most complex payment portfolios and is proven to operate reliably in some of the demanding payment environments.

About IBM Financial Crimes Insight

By resolving relationships and scrutinizing behaviors to identify high-risk entities before they commit financial crimes, IBM Financial Crimes Insight empowers institutions to increase both the efficiency and the effectiveness of their payment fraud detection, anti-money laundering compliance, know-your-customer, conduct surveillance, and insurance claims investigation programs. Only IBM uses the broadest set of market-leading AI, IBM cognitive services, big data and automation technologies, driven by input from leading regulatory experts to minimize the financial and regulatory burden of compliance while reducing reputational risk.

For more information

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