IBM Safer Payments

Preventing fraud across all payment channels

Thought leadership White paper

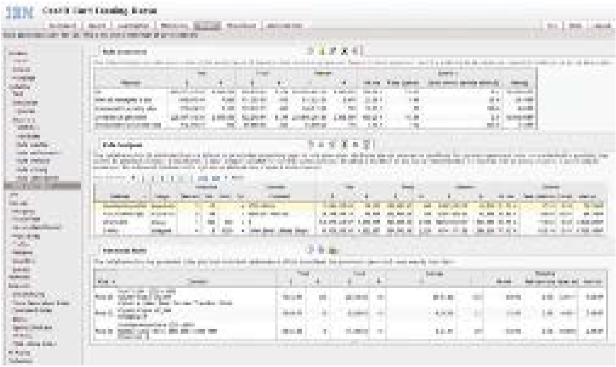
IBM Safer Payments

IBM Safer Payments is the industry's first true cognitive fraud prevention solution to payment processing and protects some of the largest and most complex payment portfolios in the world. Users 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 use 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.

Figure 1: Next generation cognitive model generator uses artificial intelligence to create decision rules.



Second generation solutions generated fraud detection models from past data. Neural networks and advanced statistics used for this typically required collecting large amounts of data over a long period of time. 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.

Second generation solutions date back from a time when fraud patterns only changed slowly, so this was not too significant a problem. In today's world, however, new patterns of fraud attack are frequently introduced and the speed of change is only accelerating. As a result, neural network vendors have thus added first-generation rules engines to their products, so that the customers can create workarounds to their aging models. This is because neural networks are black boxes; they only generated a score that cannot be explained by looking at the model. In addition, the neural network model cannot be explicitly modified. Experience shows that some users of neural network-based solutions have moved away from dependence on the model and only use the rules function to mitigate cost and erratic performance.

IBM believes that using one modelling technique to fix the shortcomings of another is a logically flawed approach. To avoid this flawed approach, next generation solutions use cognitive computing to create one clean and efficient model.

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 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.

In addition, local specialists can enhance such rules and scenarios as they are easy to read and to understand. They can also combine them with their own human experience, and perform frequent updates of the models. In fact, the automated learning is so fast and efficient that some users elect to adapt their models up to multiple times per week.

Figure 2: Manual creation of decision rules as part of rule sets.

Their experience is confirmed as providing them with a competitive advantage. This approach curbs emerging fraud patterns at the earliest opportunity while keeping false positives low.

Democratization of model generation

Second generation fraud prevention often implied that users have to ship their data off site to the vendor, who then generated a model and shipped it back to the user. Unfortunately, the black-box nature of the model prevents the user's fraud analysts from gaining any understanding how the model works. And in case it does not perform well, they have no way of explicitly modifying it.

This renders users at the mercy of their vendors. The cognitive computing approach of IBM Safer Payments' next generation product frees users from this dependency. Because users are enabled by the artificial intelligence to create their own models, they become self-contained and independent.

The proof: all users of Safer Payments are adapting their existing fraud prevention models without needing any assistance from IBM. Many have even created full day-one models for new lines of business completely independent of help from IBM.

Customer success

IBM Safer Payments today protects some of the largest and most demanding applications in the world, delivering outstanding results. COMDATA, a major US corporate card issuer has used IBM Safer Payments technology since 2007. In COMDATA's MasterCard portfolio, IBM Safer Payments reduced the fraud level from the market average 12 basis points for corporate credit cards to just two basis points1. And even more importantly, the false positive rate was reduced to just 1:3, which is only a fraction of the 1:20 to 1:40 reported by other issuers in the US.

IBM Safer Payments is also the leading fraud prevention solution for the chip and contactless card era. The first major economy that completely converted to chip cards was France in 1992. While this initiative initially reduced fraud significantly on credit and debit cards, fraud eventually returned. In fact, in 2013, the European Central Bank reported the highest fraud losses in the Eurozone for France. Since 2014, IBM Safer Payments helps protect French-issued cards and French merchants from fraud from its central installation at the National payment switch2. Sized for 10 billion transaction messages annually, a peak performance of 4,000 transaction messages per second, and a maximum latency of 3.5 milliseconds, this is one of the world's largest payment portfolios.

IBM Safer Payments also helps protect the payment systems of the future. QIWI (NASDAQ: QIWI) is the dominant mobile payment system in Eastern Europe. It operates 200,000 cash deposit ATMs, serves 75 million active account holders and processes seven billion financial transaction messages annually. Enrolling with QIWI is as easy as inserting a banknote in one of the many ATMs, entering a mobile phone number as the account number and choosing a password. The funds can then be transferred to any other QIWI user, be used at point of sale (POS) or to pay invoices. Accounts are typically accessed by account holders through their mobile phones. A system so easy to enroll and so convenient to use, naturally becomes a honey- pot for criminals. Thus, QIWI employs IBM Safer Payments to keep its easy onboarding and payment processes protected from financial crime.

These three examples are representative of many successful IBM Safer Payments implementations.

Farewell, consortium model

Neural networks and advanced statistical methods require massive amounts of training data to create a stable model that does not overfit. Frequently the amount of data that individual users can provide for this is not sufficient. Born out of necessity, neural network vendors in the 1990s created the concept of the consortium model, where they pooled data from multiple users to create models.

While this has worked somewhat well in the past, and in homogenous markets, consortium models fall short in today's dynamic environments. In small payment markets, fraud patterns are rather regional and thus blending data from multiple user results in low detection rates and many false positives. In large payment markets, fraud patterns tend to become more and more individual by user, so consortium models become less and less effective.

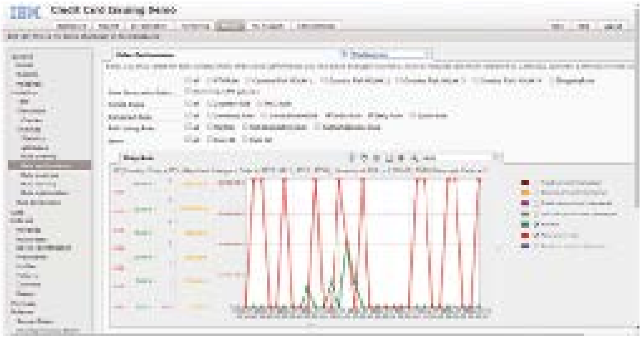
In direct comparison, the cognitive approach yields stable models with much less data than neural networks require. This means that even small or medium sized users can afford a custom model. Optimized for the fraud patterns this user experiences, a custom model generates higher fraud hit rates and lower false positives.

As an added benefit, the fact that model updates—such as adaptations of an existing model to emerging fraud patterns— require very little new data, the cognitive approach also allows to update models within days and even hours of a new fraud pattern emerging.

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.

Figure 3: Constant monitoring of fraud prevention performance highlights non-performing rules.



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 are 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 risk of merchants defaulting 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 work ow 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 section 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 by enabling 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.

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.

SWIFT and high value payments pose a unique fraud detection challenge. Fraudulent transactions in this channel are rare and barely distinguishable from genuine transactions. However, missing just one fraud is extremely expensive. Protecting these payments requires understanding each customer's normal behavior across a diverse set of parameters—some about the transaction, some about the parties, and some about the context. IBM Safer Payments is uniquely capable because the solution maintains a deep history of each customer in memory so normal patterns are readily available to the detection process. As payments are evaluated, the payment instructions are enhanced with information about the context of each payment to provide a total view. By evaluating payments across this diverse set of behaviors, even the shortest of variances from your customer's normal behavior is identified in order to stop the first fraud.

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 f light, 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.

Protecting the Internet channel

E-commerce acquirers, payment gateways and online banking face the same problem: they need to secure the identity of their counterparties. This is more complicated with Internet-generated transactions when the counterparty of the transactions— buyer or account holder—is not physically present and there is no material token such as a payment card. IBM Safer Payments is the right solution here because it provides a full set of functions to establish identity and to detect fraud with transactions originated in the Internet.

An embedded device fingerprinting and identification mechanism feeds into a device reputation database that profiles all devices each counterparty ever used. This allows IBM Safer Payments to assess whether the currently used device is in fact owned by the counterparty. At the same time, the devices themselves are profiled. If for instance a device never used before within a short amount of time is used with a number of otherwise unrelated accounts, this is an indicator of high risk.

IBM Safer Payments also extracts device intelligence. A customer may pretend to be in the UK and come in with a UK IP address, but when IBM Safer Payments identifies that the browser language is Mandarin, the time zone is Shenzhen and that this is the first time the account has been accessed with these settings, it considers this an indicator of high risk.

Also IP/ISP usage is profiled. If the counterparty uses an ISP frequently used before, this is a low risk indicator compared to using an ISP never used before. There are also know high risk ISPs and known low risk ISP. But IP/ISP are not just profiled for counterparties, they are also profiled within their own usage history. Massive attacks by organized crime are typically conducted from a single ISP and sometimes even a small set of IP addresses. A significant number of similar transactions from multiple accounts originating from a single ISP that was never used with any of these accounts before is an indicator of high risk.

Similarly, target accounts in mobile and online banking are profiled. A target account that has previously been used by an accountholder multiple times over a certain time period most likely is not linked to a fraudulent attack. IBM Safer Payments even uses social intelligence: target accounts used frequently over a time period by other account holders are not likely linked to a fraudulent attack; even if the current account holder uses such a target account for the first time.

IBM Safer Payments can also be loaded with each https request of a mobile or online session. The specifics, sequence and timing of the https request can be matched to known malware signatures. This allows for the identification of active and acting malware in a session.

Omni-channel

As previously described, IBM Safer Payments provides the channel-specific feature set needed to prevent fraud in any payment channel and any line of business. It is important to notice that most IBM Safer Payments' installations support multiple lines of business. This not only reduces the total cost of ownership, but it also allows profiling entities throughout the payment channels, and thereby to detect inter-channel fraud.

For example, if a bank's online banking accounts are compromised and the fraudsters do not immediately transfer money outside the bank. Instead, they use mule accounts within the same bank, and then use ATM withdrawals, POS transactions and e-commerce transactions from the mule accounts to take out the proceeds. Such a fraud pattern can only be detected securely when the flow of money is followed throughout the bank's silos.

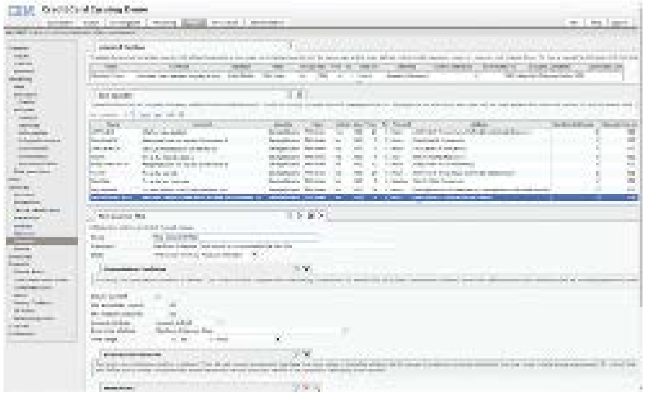
Profiling engine

The heart of IBM Safer Payments' fraud detection capability is its powerful profiling engine. It features a number of different ways to profile past behavior in any historical dimension. This enables the identification of a full past behavioral profile of a cardholder, account holder, originator, beneficiary, intermediate, merchant, terminal, ATM, POS and so forth. This profiling is fully performed in real time, which is at the time a current transaction message is processed. The result of the profiling thus becomes available to the actual decision model while the transaction is still in process.

The methods of profiling are multifold. Counters can generate a profile such as "how many times was this card used at the current same ATM in the past 72 hours where the amount withdrawn is the one most frequently withdrawn by the customer in the past three months". Patterns allow to find specific sequences of transactions and events that occurred in the past. Calendar profiles compute averages and frequencies of any type of transactions in any calendar period in the past. Collusion profiles rapidly identify common points of purchase in the past of multiple cards that were compromised. Events record specific occurrences in the past and measure how much time has passed since.

It is important to notice that all of these profiling methods are fully configurable in flight and that all data elements of all data streams can be used in their definition.

Figure 4: Powerful real-time profiling engine analyzes historical behavior of all entities.



Decision engine

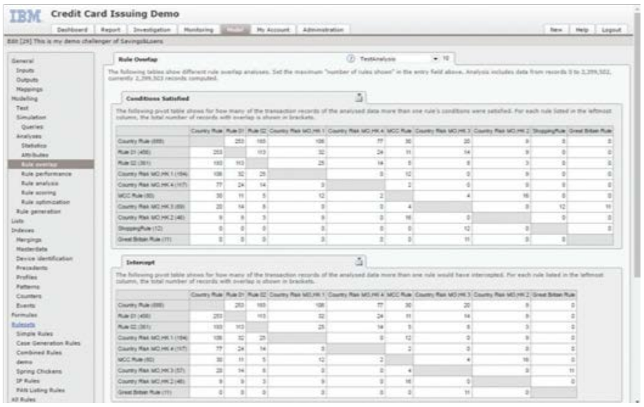
All data fields of all data streams, as well as all profiling computed data can be used in IBM Safer Payment's decision engine. The decision engine allows for the definition of rules and scenarios, structured in rule sets and scenario assemblies, and modelled in a hierarchy. Rules and scenarios both represent decisions with respect to the risk assessment of the current transaction message, as well as policies on how to act on this assessment and invoke any kind of external action.

One type of such action is the risk scoring or decision with real-time transaction messages. The authorization system or transaction platform that sends data of a current transaction to IBM Safer Payments as a message receives back information on whether to authorize this transaction or to decline it. Alternatively or in addition, this yes/no type decision is accompanied by a risk score or the estimated probability that the current transaction turns out fraudulent later on.

Decision rules and scenarios can also trigger actions in other back-office systems of a payment processor. For instance, a payout for a specific merchant can be blocked until an operator reviewed the case in the investigation workflow and cleared the account block. Decision rules and scenarios can also generate notifications about transactions to parties as emails, fax or text messages.

Another type of action is an investigation case alarm. Such alarms can be created for real-time transaction messages as well as for transactions loaded in batch files. Alarms are used to create investigation cases for various case queues and may contain individual priority scores. They can be used both in IBM Safer Payments' integrated case investigation workflow and with other case investigation tools.

Figure 5: Flexible decision model analysis tools enable generation of efficient models.



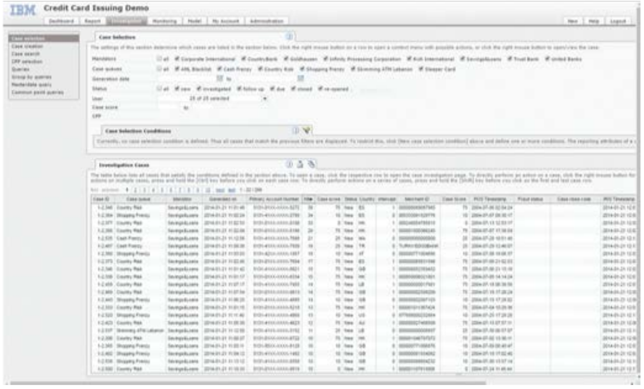
Simulation and analysis environment

IBM Safer Payments contains a complete virtual simulation testbed. This allows for each local fraud analyst using IBM Safer Payments to create any number of challenger models to the current champion. With a challenger, new and modified fraud counter measures such as profiles and rules and scenarios are created, and their effectiveness can instantly be simulated for a defined period of real production data. If the challenger outperforms the champion, it can be promoted into production to become the new champion. This entire process is governed by a revision control system that provides full audit trails and allows to exactly identify how any past decision at any time was made.

The important element here is that all these challengers are simulated within the same physical environment that performs the actual real-time decisions using virtual sandboxes. A sophisticated priority scheme ensures that no such simulation or analysis would ever consume resources needed by the real-time engine. Since in an average production situation, most of the computational resources are not used by the real-time process, free resources are generously available to perform simulations and analyses.

Because the virtual simulation on the production environment puts a data layer between the challenger and the data, any experimentation with the challengers never alters the real production data. Because the fraction of the data changed in any virtual simulation is rather small, most of the data needed can come from the production data store. This is a very efficient utilization of the production server's computational and memory resources and allows for any kind of simulation and analysis to be started with real production data to start instantly. This process is near instant and shortcuts the lengthy traditional process of data extraction, moving from production to test environment, and loading/processing it there.

Figure 6: Case investigation workflow selection function allocates alarms to investigators.



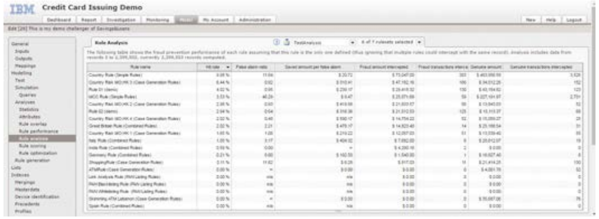
End-to-end solution

IBM Safer Payments provides a full set of functionality that supports all functions of a multi-channel payment fraud prevention solution.

A real-time decision engine executes profiling of thousands of transaction messages per second within milliseconds latency. It allows for the profiling into any historical dimension. This includes cardholder and account holder behavior, merchant/ terminal/ATM behavior, but also merchant categories, regions, IP/ISP, devices and so forth. Because these profiles can be built across silos, inter-channel fraud patterns can be prevented.

Since certain profiles require the assessment of individual past transaction records while the current transaction message is performed, IBM created a purpose-built database for Safer Payments. This database, optimized purely for the purpose of payment fraud prevention, can be of orders of magnitude faster than any generic database technology. In processing payment data and profiling behavior, users have benchmarked it to orders of magnitudes faster than general purposes database systems. This is partially from its

Figure 7: Detailed reporting on model performance.



use of in-memory and not-only-SQL technology, however, most of its performance gain comes from building it for the sole purpose of processing payments data.

The massive performance of the IBM Safer Payments' database is also the key behind its ultra-fast statistical analysis and interactive reporting capabilities. Analyses that have taken hours with general-purpose technology only take minutes with IBM Safer Payments' purpose build database.

Because this ultra-fast database technology also propels the analytical capabilities within any simulated challenger, the performance of different decision models is quickly compared, and efficient development of fraud countermeasures is provided. Because IBM Safer Payments' simulation sandboxes are virtual, any user can create any number of models and analyze/ test/develop them in parallel.

IBM Safer Payments' simulations are created as virtual data layers, so they allow for each of the decision models to access the real data and manipulate it, however, manipulated data only exists in the virtual data layer where it can be analyzed. Real data is never changed.

Because of this, simulating fraud countermeasures with IBM Safer Payments provides instant results: the virtual sandboxes are built according to any selection criteria the user defines— such as period, region or industry—and created dynamically within minutes or seconds. No need to export production data from a production environment, moving it to the test/ simulation environment, and importing it there.

All operations—real-time and others—are executed fully redundant. IBM Safer Payments uses a service-oriented architecture (SOA) and is designed to operate in a cluster of multiple, identical IBM Safer Payments instances. Within such a cluster, the instances replicate all transaction data and all configuration change automatically. IBM Safer Payments is configured and sized so that as long as there is still one instance up and running, it can take the full real-time load and all user activity. This approach to redundancy allows creation of any level of availability by just adding instances. Most IBM Safer Payments installations operate at an availability level of 99.999 percent and are using three or four instances.

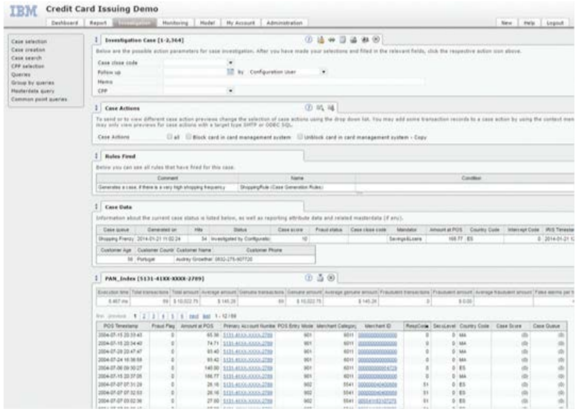
In addition to real-time reactions, IBM Safer Payments can also generate investigation cases. A completely integrated case investigation workflow is part of IBM Safer Payments. Cases can be generated for different case queues, and each case queues' reporting pages can be freely configured and customized. Cases can also be associated with a score by the decision engine for prioritization within case queues.

IBM Safer Payments' profiling engine works with a streamlined history of past transaction records that are locally stored. To create this history, typically transaction messages from various data streams are merged: settlements are merged with authorization requests, fraud alerts are merged with transaction records, and session requests are merged with payments. IBM Safer Payments comprises a f lexible and powerful merging functionality for this.

Any frontend access to data and functionalities is controlled by a configurable user role model. This allows for a refined control of access, while at the same time it enables an efficient management of hundreds of users. Interfaces to companywide user authentication systems simplify user logins.

In addition to a full query module and configurable reporting capabilities, IBM Safer Payments also features a customizable dashboard. It allows for the display of configurable alarms and the charting of key performance indicators. It also can reach out to individuals by email, text or WhatApp if certain thresholds are reached. It can also feed into centralized monitoring systems.
To document both technical and business events, IBM Safer Payments features a configurable event logging engine. Several hundred individual events can be configured to be logged for in system logs and audit trails. These logs can be locally stored and viewed within IBM Safer Payments, but also be delivered to centralized logging facilities within a data center.

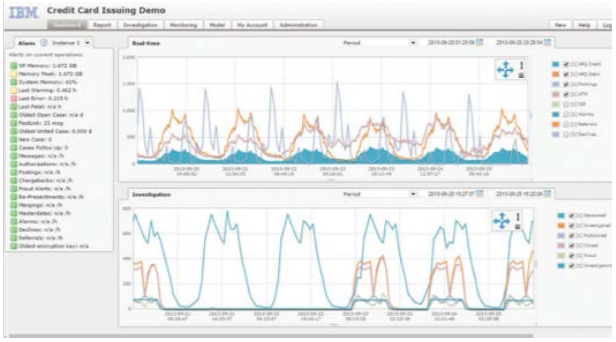
Figure 8: Investigation case reports are fully configurable for multiple case queues.



IBM Safer Payments is created for maximum scalability. While it can protect the largest payment portfolios of the world, it remains the simplest software product to install, maintain and operate.

A case in point: all binary code of IBM Safer Payments is contained

Figure 9: Configurable dashboard displaying key performance indicators and operational alarms.



in one single executable file, 15MB in size. It not only contains all business logic of all functions of IBM Safer Payments, it also contains the entire purpose build database as an embedded component. There is thus no separate database to be procured, installed, administered and patched. Because the embedded database has no parameter that must be set from the outside, there can be no misconfiguration and implementation is faster.

The single executable file also contains an embedded application server. Again, nothing needs to be procured, installed, administered, and patched. Even the entire replication logic is embedded in the single executable file. If one IBM Safer Payments instance in the cluster is taken down for maintenance or fails, once it is restarted, it replicates itself by negotiating with the other IBM Safer Payments instances and then exchanging the missing data. As a result of this, all that IBM Safer Payments needs to run is a set of servers with bare operating system. Everything else is already contained in IBM Safer Payments' single executable file.

IBM Safer Payments is designed as true 24x7 application. There are no batch or maintenance windows, all gardening tasks are spun off as parallel processes and executed in parallel to real-time operations. Even hardware/operation system maintenance, and IBM Safer Payments updates are done in flight.

Also the administration user interface is integrated. No consoles, no scripts, each IBM Safer Payments instance can perform the administration of the entire cluster, including all its instances.

It is important to note that IBM Safer Payments has been developed from ground up to support PCI DSS compliant operations. Each of its releases is also PCI PA-DSS certified. For users that operate with card data, this implies that when they undergo PCI DSS certification, they only need to present IBM Safer Payments' certificate to their QSA. Users that do not operate with card data are reassured by the fact that IBM Safer Payments is certified to comply with the most comprehensive data security standard of the payments world.

Completely configurable

IBM Safer Payments is designed to be configurable in any aspect. When IBM comes on-site to assist with an implementation, IBM consultants sit down with the clients' local specialists and as a first step, the various data feeds are identified for all the payment channels to protect. The data feed configurations are defined by simply typing them in using IBM Safer Payments' web interface, which is as easy as filling out a spreadsheet. Next, the physical interfaces are defined to the data feeds on the web user interface. For real-time interfaces, online messages that IBM Safer Payments responds to are defined in message formats, transportation layers and security properties. For batch interfaces, file formats, delivery types and import schedules are defined.

In a next step, the decision model's attributes are defined and then mapped to the data feed's variables. This abstraction layer allows for variables of data streams to be merged to a single transaction record history. It also allows merging non-financial and financial transactions. For example, in a standard card issuer application, settlement transactions (postings) are merged with authorization requests into a single transaction record. This is also the case for optional charge-backs, representments and fraud alerts. In the ATM channel, this allows for machine events to be merged with financial transactions so that certain channel-specific fraud patterns can securely be detected. In the online/mobile banking channel, session information, device fingerprints and device intelligence are merged with the financial transactions.

After the data feeds and the decision model's attributes are defined, IBM Safer Payments is primed with transaction data. Either offline from data exported from production systems, or by connecting the configured IBM Safer Payments to the data feeds themselves. IBM Safer Payments' analytical capabilities allow for an initial analysis of data structures and to define profiling. The IBM Safer Payments' artificial intelligence is used to generate a day one model that is to be used when the solution goes live. All of these steps are typically performed with the local specialists, so that they are trained on the job.

It is important to notice that all these settings can be made in flight. Even adding completely new data feeds can be done without restarting IBM Safer Payments, without a single transaction lost.

It is because of this level of configurability that implementing IBM Safer Payments is low risk and fast. Typical implementations are completed within three to six months. When implemented, IBM Safer Payments is completely adopted by the local specialists. It is typical that the local specialists do not need any support to even add completely new portfolios and lines of business.

In addition to the real-time and batch data interfaces for transaction data, IBM Safer Payments features an open API that covers 100 percent of its operational functionality as web services.

For more information

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

IBM Corporation IBM Analytics Route 100
Somers, NY 10589
Produced in the United States of America December 2019

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANT- ABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

[1] Freddy Ramirez, email message to the author, 1 March 2016.

[2] Fourth report on card fraud. European Central Bank. 2015.

Please Recycle

ASW12418USEN-01