IBM Analytics
White Paper

Preventing payment fraud: A major leap in modeling efficiency

Contents

2 Executive summary

2 A radical approach to fraud modeling

3 Creating a dual-access real-time database
- Cognitive computing: A “modeling partnership”
- The IBM Safer Payments experience
- Expert meets “expert”
- Fact-based model assessment
- Modeling in IBM Safer Payments

6 In-flight configuration
- Continuous performance monitoring
- Streamlined workflow
- Critiquing the conventional workflow
- The efficiency of IBM Safer Payments

8 Conclusion

Executive summary

To combat payment fraud, financial institutions deploy automated decision models which evaluate transaction streams in real time. If a model assesses a high likelihood of fraud for a transaction, exception handling proceeds according to predetermined business rules. While effective prevention depends on a number of operational factors, the most persistent bottleneck observed in deployed systems is the inefficiency of the fraud modeling workflow.

This white paper describes a new approach. It includes a highly distinctive modeling framework that uses cognitive computing techniques and is designed into the system architecture of a next generation fraud detection system—one that is already deployed in several of the largest and most intensively targeted payment environments. This new approach breaks the modeling bottleneck and leads to material gains in financial measures.

The streamlined workflow produces not only faster model turnaround, but does so with just a fraction of the resources required by previous approaches. Furthermore, models emerging from the workflow demonstrate material savings in decreased fraud loss accompanied by a massive reduction in false alarms.

In addition to the far improved workflow, the new approach uses compiled human expertise and is capable of proposing model improvements of its own. Acting as a “cognitive partner” the system assists skilled practitioners to implement new models faster. In this era of unprecedented evolution and automation of fraud schemes, this human/machine partnership is becoming an absolute requirement.

Ultimately, the benefits of the approach described in this white paper can go directly to the bottom line of a business by improving the effectiveness of fraud personnel and increasing operational efficiency.

A Radical approach to fraud modeling

Outthinking fraud by rethinking modeling

Over the past decade, increasingly sophisticated fraudsters are able to more rapidly scale up new fraud attacks, making them more adept at exploiting commercial payment systems. Perhaps ironically, the same technology effects that are revolutionizing payments are also revolutionizing payment fraud: fraud is steadily becoming more complex, more automated, more adaptive, and more dynamic.

An environment that used to be "merely" a bitter arms race has literally become an adaptive system that continuously kills off weaker fraud patterns and propagates stronger ones. The result poses problems for both of the two standard approaches to fraud detection:

- Statistical and neural network-based models react too slowly to track evolving fraud patterns.
- Rule-based models demand large departments of scarce expert personnel to keep models fresh and performing well on an ongoing basis.

Only a complete re-think of the modeling workflow, recognizing the need for efficient deployment of human expertise using cognitive computing techniques, can mitigate the constantly looming threat of falling behind in the race. In effect, all factors that play a role in determining the efficiency of fraud modeling must be dealt with at once. Specifically, an optimal workflow must:

- Radically speed up sample preparation time for conducting fraud pattern analysis and development of countermeasures.
- Radically reduce required intensity of effort for experts to create optimal fraud rules and statistical models.
- Radically reduce the time lag and the effort required to implement updated fraud countermeasures.
- Radically reduce the time required to discover, then either mend or remove fraud countermeasures that have lost their effectiveness.

In order to meet these criteria, the architects of the system discussed in this paper conducted a comprehensive evaluation of fraud detection technologies deployed in the field. This process led to the development of not only a new methodological approach, but several very significant new fraud processing technologies to support it.

In this paper, these advancements will be referred to collectively as *IBM® Safer Payments*.

The following sections describe the principal building blocks of IBM Safer Payments' technology and explain how they provide objectively verifiable orders of magnitude improvement in modeling efficiency.

Creating a dual-access real-time database

Within the conventional system architecture, vital access to the real-time database by the modeling and analysis function must be carefully regulated and rationed to avoid unacceptable delays in real-time transaction flow. In many cases, real-time access is not even technically possible, and only batch extracts are available. Unfortunately, for technical and workflow reasons, this operational constraint has a direct and harmful effect on model development effectiveness. Moreover, this effect becomes more and more material to the financial bottom line as the fraud environment becomes increasingly dynamic.

IBM Safer Payments, with its significant practical history in fraud modeling, went back to address the inequity of access for model generation and analytics. In the end, the solution was designed and built from the ground up to be a fully integrated fraud detection system based on an entirely novel "dual-access" real-time database engine. In this case, dual-access means that the engine supports transaction processing concurrently with fraud model analytics, development, and simulation, with no function ever needing to seek out additional resources, and no function ever finding itself blocked by the other.

Specifically, with IBM Safer Payments, model development is carried out on fresh, live transactional data. All modeling is accomplished "in-flight." Moreover, modeling and analytics are no longer separate operations in IBM Safer Payments, which is the optimal environment.

Importantly, modeling no longer imposes any penalty whatsoever on transaction processing, even in the most demanding payment environments. In fact, a savings on infrastructure is often the result of implementing IBM Safer Payments because hardware resources are used far more efficiently than in the conventional case.

As transaction load rises and falls, IBM Safer Payments elastically partitions computing capacity on a dynamic basis between real-time operations and modeling analytics. This new approach is beneficial from an infrastructure perspective, because the required data center provisioning to meet peak transaction load leaves a huge amount of processing power unused and unallocated.

In practice, most payment environments waste between 85 percent and 95 percent of computational resources during normal operations. With IBM Safer Payments, inefficient utilization for transaction processing is turned into an advantage for modeling: the same powerful computers used for transaction processing now perform routine processing of analytics, so the results of these complex operations are generally at a modeler's fingertips precisely when needed.

Additionally, IBM Safer Payments technology was designed for practical use in the field, bringing the use and power into the hands of experts. It is architected to deliver high-performance results with commodity hardware in an easily extensible, self-managing, hot-swappable cluster configuration.

Exceeding its initial design goal, with IBM Safer Payments the tracking of emerging fraud patterns based on fresh transaction data is an operational norm, instead of a vain goal rapidly receding into the distance.

Cognitive computing: A "modeling partnership"

Where IBM Safer Payments has replaced conventional fraud solutions, the single largest leap in modeling efficiency stems from the fundamentally new way models are now created.

Conventional fraud modeling uses a combination of statistical analysis, machine learning, and automated deployment of human expertise via a rules engine. IBM Safer Payments takes this base but delivers a more advanced interactive experience. Within a cognitive partnership with the fraud analyst, IBM Safer Payments uses machine learning which learns at scale, for a purpose, to deliver rules and models back to the analyst that are completely understandable and actionable. This enables optimal reaction to threats.

The IBM Safer Payments experience

Every model element in IBM Safer Payments, whether machine-derived or human defined, appears to the user as an easily readable rule, expressed in syntax and semantics natural to fraud modeling environments. In addition, IBM Safer Payments' rules for a specific payment channel can be customized to that environment.

In short, IBM Safer Payments models are optimized for readability, maintainability, modifiability, and reusability. More than anything, however, the distinction between human and machine expertise recedes into the background: rules are rules, no matter where they came from.

Expert meets "expert"

The developers of IBM Safer Payments, with decades of experience working on implemented systems, were well aware of the general unsuitability of the pure computer science approach to dynamic, unstructured decision environments.

Consequently, rather than relying on an algorithmic approach, the IBM architect team, skilled in packaging human expertise for real-time decision-making, embedded domain expertise from a cadre of seasoned fraud analysts into IBM Safer Payments. As a result, the IBM Safer Payments user implicitly partners with experts possessing deep experience garnered across multiple payment environments, all within one integrated system.

Fact-based model assessment

Of course, transparency, readability of rules, and partnering with canned experts cannot be the end goal in a system that stands or falls on its financial merits. In addition to ensuring that generated rules are as easy as possible for human modelers to understand, an integrated dashboard in IBM Safer Payments clearly lays out key benchmarks for users, including not only hit rate and false positive rate, but financial measures as well.

Modeling in IBM Safer Payments

In keeping with IBM Safer Payments' technology-as-partner philosophy, a modeling session in IBM Safer Payments can accommodate any sequence of rule development: the human expert can write rules for the system to assess analytically or the system can propose rules that the human can assess according to more subtle criteria.

Of course, expert modelers are completely free to augment, modify or ignore rules generated by IBM Safer Payments. As mentioned above, the system makes no distinction between human-defined and machine-generated rules, so the latter are fully editable. In fact, it is fully up to the human modeler how much assistance to request from IBM Safer Payments.

At each step of model generation, IBM Safer Payments suggests a next step. The modeler can accept this proposal, modify the proposal to any degree, or choose a completely different step. When a modeler chooses to accept all IBM Safer Payments proposals without modification, this is equivalent to full automation, with the profound exception that the modeler can observe the process unfold and intervene at any time.

Although this highly interactive approach is always compelling when experienced for the first time, this is not the main point. As models emerge, rule by rule, standard quality measures are calculated on the fly. In particular is the value of having the financial impact measurement also available immediately in flight.

The result is the ability to have use of completely new fraud prevention models in only a few hours, and the adaptation of existing models to newly emerging fraud patterns in only a few minutes.

In-flight configuration

In the past, fraud patterns tended not to change much over time. Fraud prevention systems thus needed updated models only every few months. In that era, downtime of a fraud system due to reconfiguration of the database, importing of a new fraud model, and so forth was tolerable since it was so infrequent.

No longer. Fraudsters are now continuously developing new fraud schemes and new variations on old themes. Once a working scheme is devised, fraudsters roll it out very quickly on a large scale. To immunize against such perils, fraud prevention models not only must be developed in radically shorter time periods, as described earlier, but also must be deployed without any interruption of service.

In some current IBM Safer Payments installations, fraud models are revised several times a day or more. This is only operationally feasible because IBM Safer Payments' dual-access real-time database permits any kind of configuration and model change in full flight. These include changes that require complete re-evaluation of past transactions, new ways of profiling behavior, and even entirely new input variables.

Continuous performance monitoring

Under today's dynamic conditions, fraud rules can become ineffective almost as soon as they are deployed. It has become imperative to be able to remove or mend rules on an individual basis as their performance declines, rather than being forced into the unpleasant decision of whether to keep using a model with declining performance or to tear it apart and rebuild.

It is highly advantageous to continuously monitor the performance of every rule individually to sound an immediate alert in case of declining effectiveness. Since all analytical components of IBM Safer Payments are tied directly into the real-time database containing the freshest transaction data, and rule performance is continuously monitored, modeling staff gain an opportunity to very quickly make a material impact on model performance as soon as it is needed: personnel are not only alerted to non-performing rules straightaway, they are also immediately presented with options to modify the rules in full manual mode, activate automated mending by IBM Safer Payments via its expert model generator, or combine the two modes, benchmark the impact, and iterate. All this proceeds, in flight, on live data, and without impact on transaction authorization time.

Streamlined workflow

As described above, IBM Safer Payments' novel architecture uniquely ties together into one integrated system all aspects of a modern fraud modeling workflow, centered on the actual, running, transaction database. Real-time transaction processing, modeling, and analytical functions are all accessible from a unified user interface within a standard web browser.

Critiquing the conventional workflow

A conventional model design workflow starts with the transfer of transaction data from real-time operations to the data repository used for model design. This data repository is typically kept separate from the real-time system to ensure that modeling never disturbs online transaction processing. Once the transaction has been transferred offline, mathematical analysis begins in order to train a statistical model, create decision rules, or both. The resulting model is then put under simulation to test its performance (figure 1).

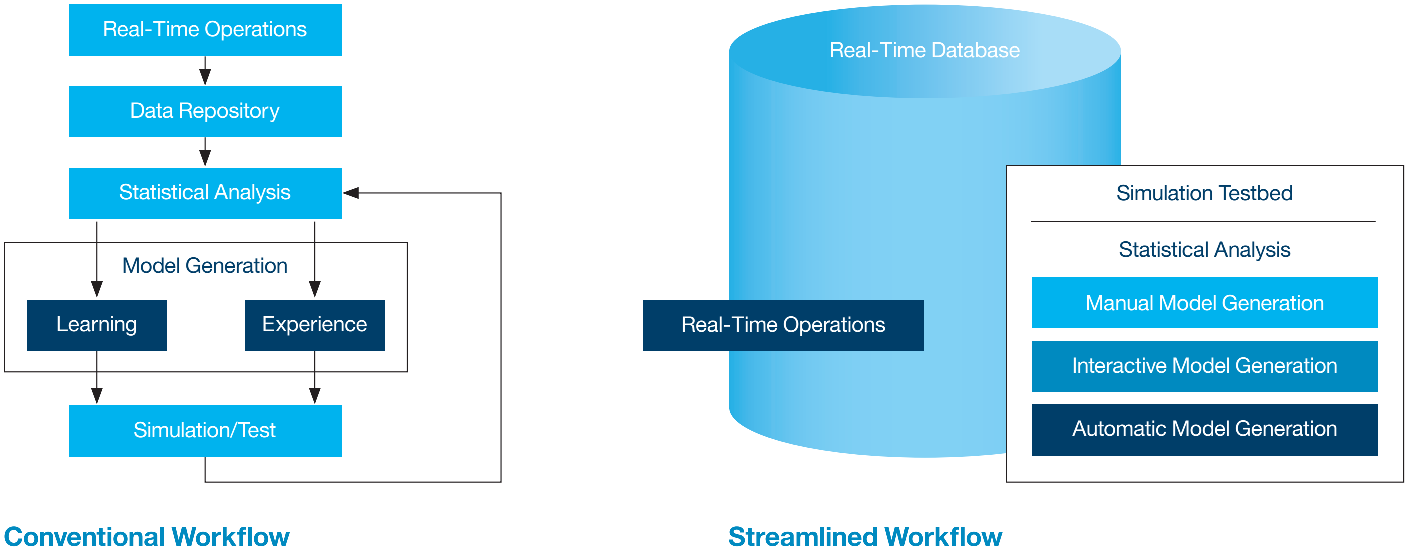

Figure 1: The differences between a typical conventional modeling workflow and the streamlined workflow of IBM Safer Payments.

Typically this process is fraught with serious inefficiencies. More often than not there are many distinct, potentially tedious steps involved in preparing the transaction data for use in modeling. Complications include ad hoc manual procedures, heterogeneous and even barely adequate tools, plus other friction- and error-prone steps.

In the end, modeling time is severely extended, resulting in a significant lag behind evolving fraud trends and, over time, increasingly suboptimal effectiveness of the model.

The efficiency of IBM Safer Payments

IBM Safer Payments offers an unmistakably streamlined workflow right from the beginning. Since IBM Safer Payments' dual-access database concurrently supports both real-time operations and modeling activity, no transfer of online transaction data to an offline repository is ever needed.

Statistical analysis and development of potential fraud countermeasures are always performed by IBM Safer Payments with full access to the running real-time system. Thus, the freshest transaction results are always available to modelers whenever needed.

IBM Safer Payments actually blurs the distinction between modeling, analysis and simulation. The IBM Safer Payments simulation testbed is also tied into the real-time database at all times, so the expert modeler gets immediate feedback based on fresh data on how the model and its components are performing. During simulation, as with all model generation phases, IBM Safer Payments modelers also have the choice to create rules manually, accept IBM Safer Payments suggestions, or simply let it automatically create a model.

Conclusion

Almost without warning, the fraud battlefield has exploded in complexity. The same spectacular technology effects that produced a revolution in payment processing also produced a revolution in payment fraud.

The community of fraudsters itself has globalized, innovating new schemes, franchising them, automating them with scripts, and disseminating them to associates in algorithm form – or selling them to their less sophisticated partners-in-crime. The line between mischievous virus creation and out-and-out theft is gone. The former abets the latter and the latter funds innovation in the former. Never before has agility in fraud modeling been more crucial – and never under such punishing conditions.

In recognizing this, the modeling experts of IBM Safer Payments – each senior team member with over 10 years of experience in fighting fraud on the ground – began a complete re-think of what 21st century fraud detection should look like. The result is IBM Safer Payments, a cognitive system that provides exactly the capabilities they always wanted in the field.

The real-world benchmarks are striking: payment processors that have moved from conventional modeling to IBM Safer Payments typically experience a loss reduction by half, while reducing false alarms by a factor of between five and 10.

For more information

To learn more go to ibm.com/saferpayments

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

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 and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, 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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle