TIBCO®

Three Ways to Drive Cost Reductions in False Positive Investigations

CUTTING THE COST OF PAYMENT OPERATIONS

The biggest headache for most payment operations teams is cost control—and a large part of it comes from fraud management (detect and investigate). All financial institutions have made huge investments in fraud systems, which often have high costs and don't deliver the expected benefits:

- Investigation teams waste large amounts of time just assembling the data needed to make decisions.
- Detection engines are always playing catchup with the latest fraud patterns.
- Ever changing regulations increase the time and cost required to reach compliance and meet audit standards.

Given their scope and impact, replacing core fraud systems is not an option for most firms. But instead of replacing them, you can improve the investigative process with augmented investigation, and improve the detection process by enhancing current systems.

This whitepaper describes three ways financial services firms like yours can use TIBCO solutions to lower the cost of investigations through faster results, reduce fraud losses through better detection, and simplify audit and regulatory compliance through centralized access to information.

1. LOWER THE COST OF INVESTIGATIONS BY PRODUCING FASTER RESULTS AND AUGMENTING INVESTIGATIONS

No matter how good a system is at detecting fraud, it will come down to a human to evaluate transactions that fall into the grey area between valid transaction and definite fraud. Here context and data are key to allowing the investigative team to make the correct decision. Typically, this means that an investigator has to manually assemble information about the customer, their habits, the transaction in question, and any related transactions. This data may be housed in multiple systems, presenting a time-consuming proposition to piece together and understand. In addition, all this information has to be logged, organized, and held so that the decision can be reviewed if necessary. Costs are further impacted by requirements laid down by regulatory bodies, where the detection process needs to be auditable and explainable, and compliance demonstrable. These constraints have often held back adoption of AI, particularly in the payments sector, because the results from ML models and their outcomes can be hard to explain and demonstrate for a regulator. But there is a solution.

One solution is augmented investigations, which brings all related data and context into a single place so investigators can make fast, accurate decisions and reference the information at any time.

SETTING THE THRESHOLD

All organizations set thresholds that trigger how to process scored transactions. Get these thresholds wrong and you either increase the number of detections (and the investigation overhead) or decrease the number of detections (and risk increased losses, fines, and customer dissatisfaction).

Rising Costs of Investigation

By far the biggest cost for organizations is the investigation of flagged transactions that fall into the grey area of validity. One way to tackle this is to flag suspicious payments via automated mobile alerts, text messages, and call systems to the card holder for verification. Alerts can have the positive benefit that customers feel protected, but they can quickly become tiresome if they occur too frequently.

Automation can only ever go so far, and eventually a human investigator has to get involved to make a determination. The overhead, which can be hundreds of dollars, is as a result of the amount of time and effort the investigator requires to make the determination. Most of this time and effort is related to data that needs to be gathered from various systems and data sources. Improving this process, by consolidating and augmenting the alert with all the relevant context ideally in a case management system, makes the process simpler and faster for the investigator, cutting costs and leading to faster resolutions.

The investigation process is also a key way to improve the detection process. Verified investigative outcomes are an essential input for new AI driven detection processes.

ML JARGON

RISK PROFILE SCORING
Detection systems use scoring. For each transaction, the system assesses the likelihood of an event being fraudulent and expresses that likelihood as a numeric score. The business then sets thresholds that determine which categories a transaction falls into based on the score. Those that have a very high confidence of being fraudulent can be handled automatically, and those that fit into the grey area and need to be further investigated are routed for human intervention. Improving the detection process enables tighter risk profiles so that more transactions are correctly identified as fraud and thus reduce the investigative false-positive workload.

TRUE POSITIVES
Transactions that are correctly flagged as fraud can be rejected (handled automatically), saving both business and customer money and inconvenience.

FALSE POSITIVES
Transactions that are incorrectly flagged as fraud are the most significant driver of cost and frustration. Results could be lack of a payment that inconveniences the customer or costly human investigation.

FALSE NEGATIVES
Some fraudulent transactions will always fall through the net. These can have the most impact, both on the business and the customer. Missing fraudulent transactions can incur hefty fines or compensation, as well as a loss of trust and ultimately business.

2. REDUCE FRAUD LOSSES WITH BETTER DETECTION

REDUCE THE NUMBER OF EVENTS TO INVESTIGATE

The second key route to cost reduction is to improve the effectiveness of your false positive management. If you get the profiles wrong or have ineffective detection, you increase the burden of investigation and/or allow too many fraudulent transactions to get through. You can improve your false positive detection rate in two ways: optimize detection systems and properly manage risk profiles.

Optimize Detection Systems

Historically, most fraud detection systems were rules based. Often built at a hefty cost by specialist third parties, these expensive systems use inflexible “black box” rules-based systems. These can be slow to update, and they miss new types of fraud as they evolve, as well. They can be expensive to buy, hard to amend, and costly to manage. Any required technical changes have significant cost due to the complexity of the rules and the testing required to prove the efficacy of the changes.

For a better solution, look for systems using artificial intelligence (AI) detection. Artificial intelligence and machine learning (ML) have given rise to new ways of enhancing the detection process. A constantly adapting AI detection system fed by the results from the augmented investigation process, allows you to be more confident that you can identify fraud as it happens and, therefore, tighten your risk profiles.

Manage Risk Profiles

This is done by enriching transactional data with contextual data in core systems and giving machine learning models more data with which to better find fraud patterns. And, these patterns are being continuously updated via a feedback loop driven by the results of the investigative systems. As a result you build more accurate, constantly refined, detection algorithms that are more effective in keeping up with the ever-changing fraud landscape.

Until very recently, AI and machine learning techniques were hard to implement, and the required skills hard to obtain. Data scientists still have a very important role to play in optimizing this new technology; However, many solutions are becoming accessible through data science platforms that simplify use of machine learning. These platforms help implement best practices and optimize algorithm selection by assisting the data scientist with things like data preparation, feature selection, and model testing.

Data is the key to building good ML models. Transactional data provides a good starting point for training supervised models, but it alone is no longer sufficient to combat ever more sophisticated fraud; it has to be augmented with other contextual data. The process doesn’t stop there. As patterns evolve, constant refinement and monitoring is required to keep models effective.

Once the models have been built, they can be deployed to run alongside traditional rules-based engines to enhance, rather than replace, the detection process.

3. SIMPLIFY AUDIT AND REGULATORY COMPLIANCE

Increasingly organizations are bound by regulations that force them to protect consumers, which also installs good business practices, but requires proving regulatory compliance and non complicity through solid auditing and logging capabilities.

Compliance requirements vary. Detection system algorithms need to be demonstrable and explainable; investigation processes need to be auditable; change control is required for rule or model deployments; and all compliance testing needs to be logged.

Each of these requirements can add expense and processing overhead without contributing to the bottom line. They are simply part of the cost of doing business in a regulated industry.

However, one of the benefits of an augmented and integrated investigative case management system, is that the system becomes the repository of all required audit and compliance data. It is the centralized holder of the who, what, and why of investigative processes needed for audit and compliance purposes.

HOW TIBCO HELPS

TIBCO's technology and data science teams have helped organizations improve their handling of financial crime, and they can help you, too. Our approach is to augment and enhance your existing systems with elements from the TIBCO® Connected Intelligence platform.

INVESTIGATION MANAGEMENT

Once events have been detected, those that fall into the grey area need to be investigated. Pushing these events into a case management system, along with all the relevant context and reasons why the model was unable to make a determination, simplifies the work of the investigator. It removes the need to search for data across disparate systems. In addition, the human determination becomes a source of training data that will improve the accuracy of ML models.

DATA EVERYWHERE

Greater amounts of data are both a challenge and an opportunity. As fraud rarely occurs in a vacuum, the ability to contextualize events with related data means that new patterns, like network analysis, find new ways that fraudsters attempt to beat the system. In addition, context is key in the investigation stage, making it simpler and cheaper to analyze, and for investigators to make a determination. Data virtualization, master data management, and data integration, all empower the detection and investigation ecosystem by pulling in contextual data on demand.

SCIENCE IN YOUR DATA

Artificial intelligence and machine learning are key to improving the detection and categorization of financial crime events. Techniques are constantly evolving, and with greater access to associated data, new ways are being found to detect fraud. Techniques like Deep Feature Synthesis that finds new data features to improve model accuracy, and tools like TIBCO's AutoML, assist both data scientists and architects to choose and test various models to find those that produce the best results.

FASTER PROCESSING

More organizations need to move to real-time operations, and this extends to the domain of fraud detection. Streams of events need to be augmented, categorized, scored, and evaluated, all in real time. This requires a combination of event processing, machine learning models, and real-time data access, all core parts of the TIBCO stack.

OPTIMIZED MODELING

At the heart of the detection system are machine learning models that are key to your success. Modeling technologies have advanced over recent years and choosing the right models can be hard. Do you know the differences between random forests and gradient machines? Can you demonstrate the effectiveness of your models? Equally important is the quality of the data; it needs to be correctly transformed and wrangled to facilitate model training, both initially and on an ongoing basis.

CONTINUOUS DEPLOYMENT

In general, IT practices are moving to more automated deployment processes, and there's no reason why you can't take advantage of this trend for your detection systems, too. The ability to train, validate, and deploy models once is good, but as model effectiveness decreases, they need to be revised and redeployed with ease in a simple auditable deployment process.

Read more about how TIBCO can help you solve fraud challenges in this in-depth technical whitepaper on reducing financial crime.

Reducing Financial Crime with TIBCO

Or **contact us** to learn more about how we can specifically help with false positive reduction.

TIBCO®

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
+1 650-846-1000 TEL
+1 800-420-8450
+1 650-846-1005 FAX
www.tibco.com

TIBCO fuels digital business by enabling better decisions and faster, smarter actions through the TIBCO Connected Intelligence Cloud. From APIs and systems to devices and people, we interconnect everything, capture data in real time wherever it is, and augment the intelligence of your business through analytical insights. Thousands of customers around the globe rely on us to build compelling experiences, energize operations, and propel innovation. Learn how TIBCO makes digital smarter at www.tibco.com.

©2019, TIBCO Software Inc. All rights reserved. TIBCO and the TIBCO logo are trademarks or registered trademarks of TIBCO Software Inc. or its subsidiaries in the United States and/or other countries. All other product and company names and marks in this document are the property of their respective owners and mentioned for identification purposes only.

04/02/19