Transactional fraud detection: A modular approach

Addressing the next generation of financial crimes

Contents

Introduction

The increasing prevalence of enterprise financial crimes has made fraud prevention and investments in prevention technology a long-overdue priority to organizations around the world. As a result, organizations are learning that the consolidated software platform approach to fraud detection is fundamentally flawed and falls short on detecting and preventing fraudulent transactions.

Instead, there are more effective ways to help fraud strategy managers and their organizations avoid the many pitfalls of deployment, deliver on the promise of holistic coverage and increase the chances of successful delivery aligned with business goals. A "one-size-fits-all" offering is unlikely to deliver enterprise-class performance with results that benefit the organization and the customer. To achieve high performance, organizations must align strategic vision with industry knowledge.

This white paper discusses the benefits of collaboration and constructively challenging the status quo by integrating different technologies to form a comprehensive fraud detection and prevention solution that meets specific business requirements. It also provides key considerations for developing a strategic road map for detecting and preventing enterprise financial crimes.

The deployed software model versus the evolution of fraud

As fraud detection professionals know, fraud is a constantly evolving organism. Like a virus, it evolves and mutates to seek out weaknesses in an incumbent detection system and, once found, will quickly exploit those weaknesses before moving—or changing—to ensure continuous income for the fraudster or organized group. Prevention methods that work today cannot be guaranteed to work tomorrow. The reality of this limitation is that deployed, packaged software applications require costly and bulky upgrades or retraining over time just to keep pace with fraud trends. The applications are only effective for a short time before they must be upgraded or replaced. Today, more effective technologies are enabled by deploying components through cloud computing and through more mature software as a service (SaaS) models.

Challenge currently deployed solutions

Fraud software today is significantly richer in feature functionality than legacy solutions. But organizations should question if their current solutions are keeping pace with the continuous evolution of fraud or if they are merely providing a richer user interface that employs the same detection routines as its legacy counterparts. For instance, one example of an ongoing problem with legacy solutions is high false positive rates (FPRs) and inappropriate transaction declines, both of which negatively impact customer service. To maintain competitive advantage, organizations must treat valued customers as such. Decisions about transactional viability should be based on sound, clearly understood logic and they should be modifiable as needed. “Black-box” detection paradigms, typically based on neural networks and other, similar, paradigms, are not the only means of providing effective fraud detection that is tempered with respectful customer service.

Finding the right transactional fraud detection vendors

It is important to note that just because it is possible to access data in a transaction system for fraud detection, it does not mean that fraud technology vendors have the ability to design a transactional fraud detection system. For instance, antimoney-laundering (AML) systems are designed to ensure compliance with regulatory requirements, not to catch fast-moving fraud. Typically, an AML system will not flag a low FPR, given that auditors and compliance resources may prefer to decline more transactions to err on the side of caution. Requiring an AML system to do the opposite and provide high-quality alerts with low FPRs is nearly impossible since the system is being asked to do something for which it was not designed. Reengineering the system for this purpose is usually ineffective.

Leverage multiple technologies to stop persistent fraudsters

Fraud is a problem that transcends individual organizations. It does not respect corporate boundaries, and fraudsters will prey on the fact that legal and technological constraints often make effective data sharing within organizations impossible. It is common to find that, after multiple fraudulent events, the same person or group has been perpetrating similar attacks concurrently on peer institutions. However, some data security vendors and storage providers act as trusted custodians that can provide access to transactional detail that shows what is happening at an industry level. As fraud or suspicious activity is identified or reported, these vendors can make data available to antifraud group consortium members to assist in catching fraudsters and closing down concurrent attacks across multiple institutions. Effective data management and security coupled with strong analytical capabilities provide the technological backbone for implementing effective detection strategies that can be shared across consortium participants.

React quickly with real-time fraud detection

Legislative, technological and competitive pressures are shortening the timeframe for reacting to fraud threats. Real-time fraud detection may be the only effective way to block fraudulent transactions. Additionally, as organizations move toward real-time capabilities, those that have not adopted this functionality will be even more exposed as fraudsters learn that a weak link exists. For instance, in the United Kingdom, real-time funds availability and the “faster payments” initiative mean that “day 2” fraud processes will become obsolete in a few years. Next-generation technology must be able to adapt and grow as market dynamics continue to change to justify any strategic investment.

Know and analyze nonmonetary fraud indicators

Nonmonetary account activity is a significant indicator of potentially fraudulent action, and yet, many organizations either ignore or are unable to capture and react to these indicators. Over time, disparate and seemingly unconnected events, or nonevents, associated with an address change request, a password change request or PIN change request can be strong indicators of account takeover or identity theft. The use of powerful predictive analytics technology and complex event processing functionality can help organizations understand the nature of their fraud problem better before the event. Organizations need the ability to assess a sequence of events or nonevents and assign a risk/threat level to that combination of activities at the front end. Preventing fraud is significantly more desirable than deploying expensive resources to manage the results of fraud—for the organization and, more importantly, for the customer. Deploying this mix of technology, analytics and human-centric knowledge can provide significant operational efficiencies, enhanced detection rates and an improved customer experience.

Base solutions on integrated technology

Effective fraud detection capabilities face a multitude of challenges across different payment methods. i.e. online, deposit, ATM, check, debit card and ACH/wire. To effectively meet these challenges, organizations must be able to move from fragmented fraud detection and prevention to an environment that is equipped to address the evolving threat of fraudulent activity in an integrated, holistic, enterprise-wide fashion. They must ask questions like: Is this technology a viable and achievable ambition for return on investment? How much depends on technology and how much on the implementation of industry and domain knowledge? What are the benefits for the organization and its customers? And in short, is it worth investing in improvement?

The answer is yes. Any organization that stops investing in technology to combat evolving and mutating fraudulent activity is effectively writing a blank check for the fraudster. However, investment in technology alone is not sufficient to mitigate fraudulent activity. Any investment must conform to a clear vision and strategy that is likely to be multiphased over several years and able to evolve over time. While packaged solutions may seem effective, as outlined in the previous section, a "one-size-fits-all" solution is destined to fail.

Look beyond packaged solutions

Fraud detection practitioners and strategists need to look beyond the capabilities provided by packaged solutions. By partnering with an external consultant, organizations may confirm that existing software capabilities and associated operational practices are adequate. If not, a consultant can also provide an effective review and recommendations for operational enhancement. Enhancement efforts should complement existing capabilities, and existing budgetary constraints, while providing a nondisruptive path to improved detection and prevention.

To implement effective fraud detection, card issuers must develop an understanding of the enhanced capabilities provided by predictive analytics, pattern and name matching / recognition, complex event processing, business rules, content analytics and, most importantly, the means for implementation. IBM's ability to draw on best-of-breed components ensures that an issuer is not tied to a specific specialization or paradigm, a key benefit when considering the specific nature of card fraud within any single geography. IBM and its broad partner ecosystem are uniquely positioned to assist institutions that are ready to begin this journey.

Conclusion

The fight against fraud is continuous and evolving at a rapid pace, and the sophistication of fraudulent attacks is ever increasing. In planning the strategy for future prevention and mitigation efforts, organizations should consider external challenges and whether their current solutions are able to address those challenges. New technologies can provide more effective ways to monitor and detect fraud and better position the organization for success. While examining different solutions, it is important to develop an understanding of the underlying detection logic.

The most effective solution sets are those that can adapt quickly, offer industry and enterprise breadth, can function in real-time and monitor cross-channel activity.

IBM's approach to fraud detection and prevention is aligned and effectively executed through the technological and commercial vision that IBM customer and business partner FIS offers. FIS' depth of experience and acquisition strategy, which includes Certegy and Metavante among others, ensures that its core offerings are infused with ideas and best practices from different, but aligned, industries.

For more information

For more information about fraud detection solutions from IBM, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**

For more information about fraud in the United Kingdom, visit the UK Cards Association at theukcardsassociation.org.uk/

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

About the authors

Richard Collard
IBM Worldwide Subject Matter Expert
Transactional Fraud Detection, AML and Risk Management
richard.collard@uk.ibm.com

Richard Collard comes to IBM as part of the acquisition, in 2009, of ILOG. He draws on a business-based career with major global fraud analytics organizations and specializes in the provision of fraud detection solutions and consulting for credit and debit card issuers and for AML. Prior to joining ILOG, he worked to develop a radical, new approach to rules-based fraud detection through the automated generation of rules using genetic algorithms and evolutionary computing techniques. This technique is holistic and non-prescriptive, espousing the belief that there is no such thing as a "one-size-fits-all solution," and is aligned with IBM's modular approach to the challenges facing the card industry.

Richard's operational reviews for card issuers in South Africa have generated significant savings and operational efficiencies. They have also been instrumental in the recent adoption of business rules management systems (BRMS) technology as a major component of a hosted fraud detection solution. Richard's ability to draw on global experience allows significant knowledge transfer of global best practices. His approach is consultative and respectful of geography and culture, ensuring that the thought-leadership that he provides is positively received—traits that have earned him significant respect through his engagements.

Aaron Calipari
Director, Product Strategy
Transaction Risk Products
Risk, Fraud and Compliance Solutions
www.fisglobal.com

Aaron Calipari is Director of Transactional Fraud for FIS, where he is responsible for risk and fraud management and profitability solution strategy and delivery. Calipari has successfully managed one of the original, commercially available fraud case management software packages while executing a strategy to bring innovative new enterprise fraud case management capabilities to market. He co-developed and currently manages a check fraud prevention service that has repeatedly outperformed traditional fraud detection methods by combining bank data with industry data sources and analytics.

Prior to his role in account management solutions, Calipari was a member of an elite team of market-focused solution strategists charged with bringing next-generation risk management capabilities to market through integration with various FIS technologies. His interest and deep domain expertise in fraud has been applied to improve performance in the areas of credit card, check and mortgage fraud.

Calipari holds a bachelor's degree in marketing from the University of South Florida.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
June 2011
All Rights Reserved

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.

♻ Please Recycle