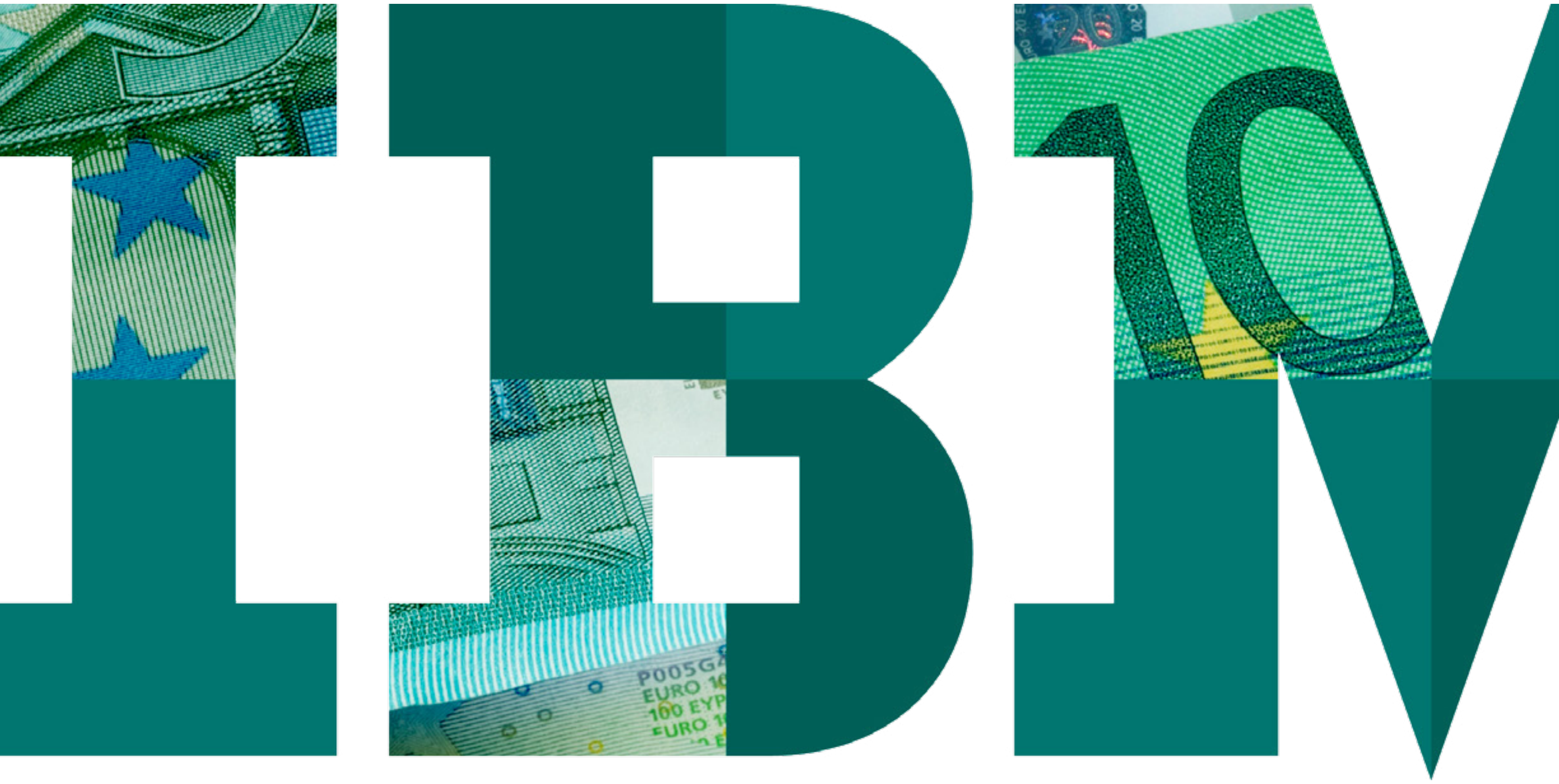
Fighting fraud in banking with big data and analytics

Reduce fraud costs and improve customer satisfaction with next-generation technologies



Contents

Fraud and financial crime can no longer be an acceptable cost of doing business. Fraud schemes are growing more sophisticated, the costs are getting higher and customer expectations are ever-increasing. In addition to triggering financial losses, fraud drives significant investigative and legal costs, erodes consumer confidence and devastates brand image. To meet these challenges, the banking industry is fighting fraud in new ways using big data and analytics capabilities.

New threats require new thinking

Every journey starts with a plan. You wouldn't start a car trip simply by getting behind the wheel and driving; you have a destination in mind. You've thought about how you'll get there, what route you'll take and when you want to arrive. You may encounter detours or take side trips along the way. But your destination is clear.

Banks are challenged daily by direct financial losses and indirect costs stemming from a growing incidence of fraud and financial crimes. One factor is the explosion in global connectivity that has provided malicious insiders and organized criminals with greater opportunities to perpetrate more frequent and complex schemes. Financial organizations are also moving to cloud computing, mobility and enterprise social media, which can add to the vulnerabilities. The old method of responding to attacks and fraud well after the fact is untenable in this new world of sophisticated financial crimes.

Shareholders and customers the world over are increasingly sensitive to the impact of fraud. The costs can include long-term erosion of brand value and customer trust, with customers often switching banks when fraud occurs. In addition, customer satisfaction can suffer due to inconvenience caused by fraud operations. For example, false positives may result in legitimate customer purchases not being approved. Organizations must strike the right balance between safeguarding data and delivering a consistently engaging customer experience.

Attackers are continuously improving their techniques and evading detection by taking advantage of disconnected security processes and technologies. In response, many financial organizations have deployed a number of point solutions to address each new threat. This security sprawl results in unnecessary complexity involving many disconnected solutions that do not provide protection across the threat landscape. Forward-thinking leaders are adopting a more comprehensive, integrated approach to the problem.

The new way to fight fraud and financial crime

Too many organizations remain vulnerable to fraud and financial crime because they aren't taking advantage of new capabilities to fight today's threats. These capabilities rely heavily on new and improved big data and analytic technologies that are now available.

With these technologies, banks can manage and analyze terabytes of historical and third-party data—far more than they ever could before. The ability to analyze massive data volumes enables banks to create highly accurate predictive models for recognizing and preventing future fraud. Organizations also require big data capabilities for analyzing streaming data in real time. Using this technology, banks can analyze transactions as they occur, detect fraud as it is happening and stop it before it causes serious damage.

Fraud by the numbers

Organizations are paying a high price when their systems are attacked and financial crimes are successful. Plus, the reputational costs can be greater than the initial financial losses.

Almost USD4.7 trillion – Projected global cost of fraud[1]

71% of customers are somewhat likely to switch banks due to fraud[2]

65% of customers would never or are very unlikely to do business again with a company that experienced a data breach where financial data was stolen[3]

85% of shoppers tell others about their experience after their information is stolen through a security breach[4]

By adopting a comprehensive counterfraud approach, leveraging the latest advancements in robust analytics, organizations can confidently protect themselves and their customers while growing the business. Potential business benefits are substantial, including lower cost of addressing fraud through automation and earlier detection, improved operational effectiveness without increasing staff and confidence in meeting regulatory compliance obligations.

Four essentials of an effective program

An effective enterprise program includes the following key phases of counterfraud measures (see Figure 1).

Detect: Predict fraud before it happens

Advanced analytics should be applied to all strategic fraud data to predict whether an action is potentially fraudulent before losses occur. Looking at only small sets of security data, such as event logs, reduces a bank's ability to prevent or detect sophisticated crime. The more volume and types of data an organization can analyze at greater velocity, the greater the success against internal and external threats.

Respond: Apply new fraud insights

Today's streaming analytics technology allows banks to gain insights and take action in real time—when it matters most. Organizations can confidently differentiate legitimate actions while preventing or interrupting suspicious actions by responding immediately to criminal patterns and activities.

Investigate: Turn fraud intelligence into action

Intelligent investigation of suspicious activity requires performing and managing inquiries that are supported by thorough analysis and information accessibility. With these tools, banks can more quickly confirm fraud so that actions such as prosecution, recovery and placement on watch lists can be taken.

Discover: Leverage existing historical data

Many banks have a treasure trove of historical data that can now be unlocked using big data analysis. They can search this data for patterns of fraud and financial crimes, and then apply the patterns to current activity. Banks can also leverage the large amounts of data gathered by industry-wide intelligence groups.

Detect
Respond
Investigate
Discover

Figure 1. The four key elements of an enterprise counterfraud program.

Moving strategically to enhance counterfraud measures

In addition to capitalizing on new big data and analytics capabilities to fight fraud, leaders in banking are also elevating the counterfraud agenda within their organizations. The complexity and gravity of managing fraud and financial crime requires organizations to look beyond their IT, operations and security teams for answers. Counterfraud must be a focus of leadership at the highest levels, including the development of a culture of proactive vigilance.

Best practices for counterfraud leadership include:

- Conducting regular threat assessments and security audits to determine vulnerabilities
- Developing contingency plans to address the consequences if a breach occurs
- Establishing a security risk baseline and future goals
- Initiating a corporate mandate that includes communications, internal compliance and a robust management system to track effectiveness
- Adopting a multilayered counterfraud model

Because threats can come from anywhere, banks need multilayered protection and detection to enhance threat visibility and prevention. The first layer in this model is designed to preemptively stop breaches from occurring. If remediation becomes necessary, state-of-the-art tools can help maintain control.

The next layer is the implementation of a comprehensive counterfraud process, employing a wide range of analytics—behavior, content, context and social network—to extract deeper insights, develop actionable intelligence and invoke automated responses. Visualization techniques that graphically depict contextual correlation enable additional insights that can be processed by human analysts. Entity analytics for uncovering the true identity of individuals and groups should also be part of the counterfraud process.

Layering of deep analytic techniques improves the accuracy of suspicious transaction detection for fewer false positives and false negatives. Analysts and investigators can then focus on actual instances of fraud, helping to improve productivity. Facilitating a collaborative investigation and case management process also helps increase the efficiency of a counterfraud program. These measures can enhance the effectiveness of big data and analytics and the ability to deliver optimal experiences for legitimate customers while proactively countering fraud.

Spotlight on success: Adding big data and analytics to fraud detection

A global money-transfer company with 230,000 locations in 190 countries faced pressure to keep up with fraud and compliance regulations affecting the international business landscape. It needed to detect and prevent transfer fund fraud before it could impact the company's customers.

By incorporating big data analytics into its fraud detection efforts, the company:

- Increased its ability to identify and interrupt potentially fraudulent transactions by 40 percent
- Prevented thousands of customers from losing funds to fraud and realized a 72 percent reduction in consumer fraud complaints in one year
- Stopped more than USD37.7 million in fraud

A South American bank needed to adhere to stricter governmental reporting requirements. To meet these regulations, the bank needed to analyze millions of daily transactions to identify current and potential fraud.

By using data mining to identify potentially fraudulent transactions, the bank has the tools and insight it needs to:

- Detect and analyze patterns of more than 1.3 million transactions a day, an 80 percent increase in analysis productivity
- Deliver a 40 percent increase in identifying suspicious transactions and a 200 percent increase in reporting capabilities
- Prevent and report potentially fraudulent banking activities that may stem from criminals and terrorists

Why IBM?

IBM is ideally qualified to deliver an improved approach to anticipating, preventing and resolving organized and opportunistic fraud. Its multilayered approach leverages a strategic vision, technology and expertise. This approach brings together IBM's continuous investment in technology, some of the latest advancements in robust analytics, and broad and deep industry and business expertise, all to protect the enterprise and its customers in the fight against fraud and financial crimes.

With industry-based business outcomes from more than 100 annual fraud consulting engagements, IBM can deliver results at the point of operation by integrating analytics with operational decision making. Able to tap into more than 500 global fraud experts and the expertise of 15,000 strategy and analytics consultants, IBM also provides robust program management. These resources help define and support the rollout of enhanced counterfraud prevention strategies across the enterprise, while IBM continually seeks opportunities to leverage clients' existing infrastructure for maximum business value.

A comprehensive set of solutions

IBM offers a full set of solutions integrated with big data and analytics that support today's new approach to counterfraud management. Together, these solutions help protect against even the most sophisticated fraud and financial crimes.

- IBM Counter Fraud Management: Integrated solution with systems and processes to manage the entire fraud and financial crime process, including predictive analytics, identity analytics, enterprise fraud management, business intelligence, case management and content analytics
- IBM® PureData™ System for Analytics: Data warehouse appliance that speeds the analysis of fraud data to improve models and fraud detection
- IBM InfoSphere® BigInsights™: Enterprise-class, Hadoop-based system to land, store and analyze large amounts of multi-structured current and historical fraud data
- IBM InfoSphere Streams: Stream computing solution for analyzing data in motion to provide real-time fraud detection

Changing the game in fighting fraud

For smart organizations, fraud is no longer treated as a point solution. It is more than a "score." It is seen as preventable, predictable and provable, and is managed pervasively across the process lifecycle. The detection and prevention of fraud is undergoing dramatic improvement through the use of game-changing big data and analytics capabilities.

Banks can get started by establishing a big data and analytics platform to ensure trusted fraud data for analysis. The next step is to implement a fraud management solution with integrated systems and processes to manage the entire fraud and financial crime process. Capitalizing on advances in big data and analytics, banks can analyze larger amounts of data for greater insight and speed analysis to detect fraud before it impacts customers.

For more information

To learn more about how to reduce fraud costs and improve customer satisfaction, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/counter-fraud/solution/index.html

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2014

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.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

[1] Association of Certified Fraud Examiners. “Report to the Nations: Occupational Fraud and Abuse.” 2014 Global Fraud Study. www.acfe.com/rttn-summary.aspx

[2] BusinessWire. “Entersekt Poll: Banks Risk Shattering Customer Trust with Lax Stance on Fraud.” August 22, 2013. Survey conducted by Harris Interactive on behalf of Entersekt. www.marketwatch.com/story/entersekt-poll-banks-risk-shattering-customer-trust-with-lax-stance-on-fraud-2013-08-22

[3] SafeNet, Inc. Global Customer Sentiment Survey. July 30, 2014. www2.safenet-inc.com/email/2014/dp/GlobalCustomerSentiment/index.html

[4] Interactions Marketing. “Retail’s Reality: Shopping Behavior After Security Breaches.” June 2014. www.interactionsmarketing.com/retailperceptions/2014/06/retails-reality-shopping-behavior-after-security-breaches