

IBM Counter Financial Crimes Management for Banking

Detect, Respond, Investigate and Discover



Highlights

- Identify fraud before unnecessary fraudulent deposits, withdrawals or transfers occur
 - Reduce the volume while increasing the quality of alerts (false positives/false negatives)
 - Uncover complex, suspicious cross channel / product schemes sooner
 - Quickly distinguish fraudsters from your valued customers
 - Improve the effectiveness and efficiency of analysts and investigators
 - Reduce losses and minimize the impact to the customer experience
 - Meet regulatory compliance obligations
 - Employ enterprise intelligence to continuously adjust operations and stay ahead of trends
-

Fraudulent schemes are increasing in sophistication and frequency. Criminal organizations are global, professional, and experts at monetizing stolen information. They are early adopters of technology and employ a dynamic agile business model. It is therefore incumbent for financial institutions to base their counter fraud operations on technology and processes that can both scale to handle the volume of occurrences, and are flexible and responsive to react, and continuously adapt, to new suspicious patterns and schemes.

The IBM® Counter Financial Crimes Management for Banking solution is designed to help financial institutions prevent and intercept attempted fraud while detecting, identifying, and building the case against past fraudulent activity and improper payments. Looking at counter fraud operations as an entire lifecycle, this IBM solution introduces advanced analytics and investigative analysis throughout the entire process. Implementing this holistic approach can translate into lower fraud losses and operational costs, while improving business results and supporting a superior customer experience.



A paradigm shift how Financial Institutions can combat fraud

Traditionally, observation spaces for banks have existed in silos. Business units including Cards, Lending, and Deposits, have separate teams looking vertically at their channel or product with point solutions.

These business information silos create critical intelligence gaps within the organization. Without interdepartmental intelligence and communications, suspicious activity and fraud patterns can remain undetected. In addition, disconnected and niche fraud solutions increase overall operating costs and resource needs.

The IBM Counter Financial Crimes Management helps bridge these gaps by building an ecosystem of tightly woven capabilities that use big data and entity analytics to eliminate information silos, expand the observation space, and enable unified enterprise business intelligence. Designed for the lifecycle of tracking and resolving fraudulent activity, IBM Counter Financial Crimes Management delivers strong insights that enable proactive and anticipatory decision making within the four operating components of *Detect*, *Respond*, *Investigate* and *Discover*. (See Figure 1.) meets the needs of all lines of business across the enterprise, and provides the SIU/FIU groups with the ability to harness a deep set of unique analysis capabilities.



Figure 1: The IBM Counter Financial Crimes Management Solution for Banks takes an enterprise approach.

Operating components include:

Detect: Apply Know Your Customer (KYC) analytic models, scoring and rules to determine if a 'customer action' is potentially fraudulent. Utilize intelligence from past discovery and investigation processes to recognize fraudulent activity patterns and highlight them for further investigation by the investigations team.

Respond: Confidently differentiate legitimate actions while preventing, or interrupting, suspicious actions by responding immediately to criminal patterns, activities, and intentions. A quick response encourages criminals to seek an easier target.

Investigate: Perform and manage the detailed inquiries into suspicious activity that will support the compilation of evidence and provide the thorough analysis required to build more compelling cases for prosecution and recovery, or denial of payment. Leverage an established governance process for validating new rules, models, and watch lists that are crucial to the feedback loop in the fraud management lifecycle, helping to address dynamic changes in fraud schemes.

Discover: Leverage a rich set of analytic capabilities to identify suspicious activity by retrospectively reviewing historical data, analyzing patterns and building watch lists to identify individuals or organizations that might be conducting fraudulent activities.

IBM Counter Financial Crimes Management provides a holistic, end-to-end approach

IBM Counter Financial Crimes Management delivers all components in one, advanced fraud solution for the enterprise. Robust dashboards provide a concise, overall view of the fraud management process. System reports enable analysis of existing and potential exposures and the effectiveness of current procedures.

You can also proactively assess the impact of changes to operations and productivity. Visualizations depict contextual correlations that help team members gain deeper fraud insights. IBM Counter Financial Crimes Management employs multilayered analytical techniques throughout the observation space. Rich analytics extract insights, develop actionable intelligence, and invoke automated response capabilities using leading market analytics tools, as listed in Figure 2.

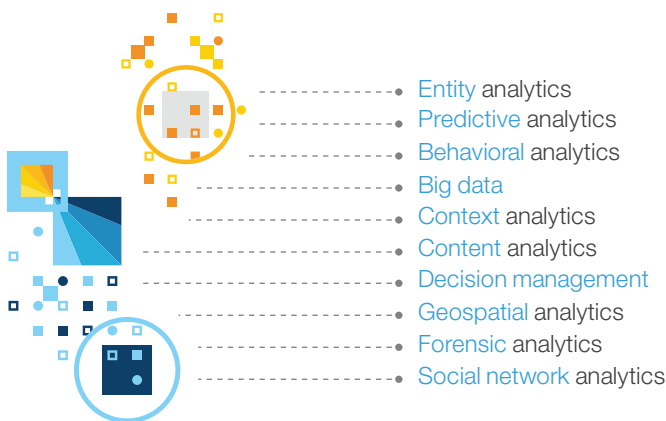


Figure 2: The IBM Counter-Fraud Solution for Banking offers rich analytical and decision-making capabilities.

Fraud threats and schemes are continuously evolving. Financial institutions must stay vigilant, constantly monitoring and adjusting their models and responses. Merging individual rules, analytics, and techniques into a seamless, end-to-end operation will enable the organization to have deeper insight and react with more confidence.

With IBM Counter Financial Crimes Management, forward-thinking organizations can proactively combat fraud, improve business results and reduce loss while maintaining a positive customer experience.

For more information

To learn more about IBM Counter Financial Crimes Management, visit ibm.com/smartercounterfraud or, contact your IBM representative.



© Copyright IBM Corporation 2014

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2014

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

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 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.



Please Recycle