Fighting Fraud in Financial Services: A Guide to Choosing the Right Technology Solution

Abstract

Fraud detection and prevention pose a big challenge to the financial services industry. Banks and financial institutions typically invest significant time and resources on combating fraud and financial crime. A key component of these programs is the software solution used to monitor, detect, and report suspicious or fraudulent activity within financial institutions. This paper highlights the critical factors that must be considered in selecting the right fraud solution for fraud control.

The Evolving Fraud Landscape

In response to the rising customer demand, banks and financial institutions are investing heavily in enabling digital services through multiple channels. This has expanded the attack surface and created new vulnerabilities that fraudsters exploit by employing sophisticated fraud tactics.

Banks' fraud detection and prevention solutions, on the other hand, are unable to keep pace with fraudsters' shifting techniques as evidenced by the rapid rise in cybercrime in the financial services industry. In addition, enforcing proper business conduct and ensuring adequate internal supervisory procedures and systems to control fraud are key imperatives for banks, failing which they are liable to be fined heavily (some such instances have been listed below).

- The Citigroup was fined over $10 million by the Securities and Exchange Commission (SEC) over inaccurate books and records, inadequate trader supervision, and poor internal accounting controls. Lack of adequate controls to verify invoices and documents submitted by a borrower resulted in Citigroup losing around $475 million.[1]
- The US Department of Justice has charged 15 individuals in a multi-million dollar international money laundering and fraud scheme. Bank accounts opened in the names of shell corporations were used to perpetrate the fraud of approximately $94 million.[2]
- The US Department of Justice has imposed a civil penalty of $2.09 billion on Wells Fargo under the Financial Institutions, Reform, Recovery, and Enforcement Act for originating and selling mortgage loans containing misstated income.[3]

Clearly, financial institutions must make a step change in the way they approach fraud detection and prevention. What is required is a change in the mindset – to embrace risk by adopting next-gen solutions based on Big Data and analytics, artificial intelligence (AI), and machine learning (ML) algorithms besides establishing and enforcing strong supervisory controls. Equipped with real-time detection capabilities, such solutions will enable banks to respond quickly to suspicious activities, proactively prevent fraud, and control and manage financial risk more efficiently. However, not all solutions available in the market incorporate out-of-band (OOB) capability or utilize ML and AI technologies.

Emerging Trends in Fraud Detection and Prevention

Banks are moving away from standalone fraud detection and prevention systems to enterprise-wide predictive risk assessment frameworks that incorporate analytics and real-time detection capabilities. Some emerging trends driving next-gen approaches to fraud detection and prevention include:

Centralized data repository

Banks are establishing centralized data repositories with data spanning customer accounts and transaction data from multiple channels and product systems as well as external sources such as social data. By leveraging high performance computing technologies, banks are analyzing massive amounts of data in real time and building comprehensive profiles of customers that can be utilized for investigation of money laundering and fraud as well as for surveillance operations.

Real-time detection

Adoption of fraud solutions that enable in depth analysis of internal and external data for real time fraud identification is gaining traction. Entity analytics and graph visualization techniques are used to detect underlying patterns and anomalies that exist in data.

Predictive fraud models

Rule based fraud identification is being augmented by sophisticated predictive fraud models fueled by analytics on enormous amounts of data. To enhance the predictive capabilities of the model, advanced analytical techniques such as pattern analysis to identify anomalous behavior and link analysis to detect hidden frauds are being leveraged.

Enterprise case management

Banks are leveraging enterprise case management to improve the efficiency of investigation workflows. Data visualization tools for faster decision-making and robotic automation for optimal business processes are other common trends being seen.

Next-gen authentication mechanisms

Innovative, secure authentication mechanisms that do not impact customer experience are being adopted. Banks are employing a variety of authentication mechanisms that seamlessly verify customers' identity through multiple techniques such as voice and speech analytics, desktop analytics, and so on.

Making the Right Choice: Evaluating Solution Options

Implementing the right solution is key to financial crime prevention. The core solution engine is a key enabler in ensuring effective detection and reporting of fraudulent activities to regulators. Thus choosing the right fraud solution vendor after a thorough evaluation of critical organizational factors and business requirements assumes importance. Based on our experience of working with multiple global clients, we have identified some key capabilities that must be part of a futuristic fraud detection and prevention solution (see Table 1).

Category	Sub-Category
Market potential	Industry experience
	Customer support and professional services
	Pricing model
Technology coverage	Security and controls
	Scalability and performance
	Infrastructure compatibility
	Product and services coverage
	Advanced analytics
	Data and analytics platform
Functional coverage	Scenario coverage
	Historical data migration
	Upgrade methodology
	Reporting coverage
	Multi-geography support

Table 1: Capabilities of an Effective Fraud Solution

Evaluation methodology

In our view, a holistic assessment must map vendors' capabilities to the capabilities listed in Table 1 and evaluate them against the key criteria shown in Table 2. In addition, based on multiple consulting assignments, we have assigned weightages to demonstrations (proofs of concept) basis the first four criteria in Table 2. However, these criteria and the weightages can be customized to suit individual bank's priorities.

Criteria	Rationale	Mode of assessment	Weightage
Organizational alignment	Suitability of the organization and its strategies, policies and systems to the bank's landscape	Demonstration and questionnaire	10
Requirement fitment	Ability to support key functional areas and meet the identified capability requirements	Demonstration and questionnaire	30
User experience	Quality and consistency of the user experience	Demonstration and questionnaire	10
Technical fitment	Technical capabilities spanning infrastructure architecture, security and compliance, as well as the efficacy of service levels and support	Demonstration and questionnaire	20
Total cost of ownership	Total investment needed for the software, hardware, hosting, support, maintenance and updates over a five-year period.	Questionnaire	20
Client references/ track record	Insights from client references	Calls to clients	10

Table 1: Capabilities of an Effective Fraud Solution

Individual banks must define the criteria for selecting the right vendor based on their specific organizational priorities. Assigning weightages to important product features and functionalities ensures a holistic assessment of vendors' capabilities. Quantitative scoring of qualitative information helps banks rank different vendors' products and facilitates the selection of the right product.

The Bottom Line

The implementation of a next generation fraud solution will deliver myriad benefits such as reduced total cost of ownership, enhanced staff productivity, and visibility into fraud exposure, besides helping firms to protect their reputation and brand. Fraudsters, however, will always find new ways to commit fraud; selecting the right fraud solution thus becomes a critical component of the larger financial crime compliance program. Choosing the right vendor will require banks to undertake a comprehensive evaluation process spanning current state assessment and demonstrations from vendors based on operational, domain, and technical requirements to help evaluate and identify the vendor to partner with. Financial institutions must therefore adopt solutions capable of handling emerging fraud trends to reap substantial returns on investment.

References

1. US Securities and Exchange Commission, Citigroup to Pay More Than $10 Million for Books and Records Violations and Inadequate Controls, Aug 2018, Nov 2018, https://www.sec.gov/news/press-release/2018-155-0
2. US Department of Justice, Fifteen Individuals Charged in Multi-Million Dollar International Money Laundering and Fraud Scheme, Oct 2017, Nov 2018, https://www.justice.gov/usao-sdfl/pr/fifteen-individuals-charged-multi-million-dollar-international-money-laundering-and
3. US Department of Justice, Wells Fargo Agrees to Pay $2.09 Billion Penalty for Allegedly Misrepresenting Quality of Loans Used in Residential Mortgage-Backed Securities, Aug 2018, Nov 2018, https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-209-billion-penalty-allegedly-misrepresenting-quality-loans-used

About The Author

Anirudha Jadhav

Anirudha Jadhav is a domain consultant in the Financial Crime Compliance (FCC) group of TCS' Banking, Financial Services, and Insurance business unit. With over 12 years of industry experience, he is responsible for thought leadership, strategy consulting, solution design, and innovation in the area of FCC for several of TCS' BFSI clients in North America. Jadhav is also responsible for building solutions, frameworks, consulting, and pre-sales support. He holds a Bachelor's degree in Computer Science Engineering from Shri Guru Gobind Singhji College of Engineering, Swami Ramanand Thirth Marathwada University, Maharashtra, India.

Contact

Visit the Banking & Financial Services page on www.tcs.com

Email: bfs.marketing@tcs.com

Blog: Drive Governance

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty. IT Services
Business Solutions
Consulting

TCS Design Services I M I 1 I 1 I 18