The Vital Triad for Fraud Prevention: Horizon Scanning, Analytics, and Machine Learning

Abstract

Financial institutions have evolved into multifaceted organizations with diversified operations, complex products, multiple channels, and a diverse workforce including multiple vendors. This massive ecosystem has increased the vulnerabilities within the people-process-technology triad necessitating a robust fraud prevention mechanism. In addition, as regulatory and compliance requirements become more stringent than before, financial firms need an intrinsically intelligent, multi-pronged approach to fraud prevention. We believe horizon scanning, analytics, and machine learning to be three key tenets of a robust fraud prevention mechanism. This paper explores how banks and financial services firms can apply the 'vital triad' to improve the ability to embrace risk and adopt new or unexplored operating models, thereby creating value for customers and partners in addition to their businesses.

The Rocky Road to Fraud Prevention

Fraud management is a tricky area for financial services firms. While on one hand, divisive technology landscapes add to the complexity in preventing fraud, tightly integrated systems backed by opaque and inefficient processes are no good either. Early detection of fraud and a clear understanding of fraud schemes are key to its prevention.

Historically, the focus was on continuous, real-time monitoring of systems and their applications to detect malicious activity. Analytics at best was used for deriving 'trends' from the voluminous, siloed historical data sets. However, given the increasing 'creativity' of fraud perpetrators, we believe that analytics and machine learning aided by a horizon scanning program can go a long way in identifying fraud schemes and their manifestation.

For example, a settlement fraud could span across the bank, the settlement agency, custodian, and the broker firm in between. Moreover, the fraud will typically span processes and departments in the bank, possibly even geographies. Combating such instances using traditional methods is a long-drawn process, with an expert committee evaluating the fraud scenario and initiating possible remedial action. In case, it's a first-of-its-kind fraud for the bank, this process will take even longer, meaning that precious time is lost in containing damage and preventing further incidence.

To top this, fraud prevention teams have fewer resources equipped with the multiple skills required of them. For proactive, real-time fraud identification, quantification, and prevention, banks must leverage automation tools powered by intelligent technologies like machine learning and analytics in coordination with horizon scanning techniques.

Taming the Unknown with Horizon Scanning

Horizon scanning is a systematic examination of information to identify potential threats, risks, emerging issues, and opportunities. It enables better preparedness and the incorporation of mitigation measures into the strategy and policy making processes to prevent exploitation of vulnerabilities by malicious actors. Horizon scanning data includes both soft data (opinions, collective insight, and intelligence) as well as hard data (structured transactional data, usually from 'systems of record').

With more and more processes getting digitized, banks need to connect 'systems of engagement' with their 'systems of record' to be able to detect frauds at the connective tissue level. Banks

must collectively host such data on the cloud; this will help aid their fraud prevention efforts besides delivering enormous cost savings.

With algorithms controlling our financial life in many ways, the detection of connective tissue disorders leading to frauds, is imperative.

A key feature of horizon scanning is the ability to spot the unexpected, through the use of exploratory forecasting. A study of known patterns through scenario analysis and normative forecasting should be complemented by horizon scanning techniques, which often involves spotting trends, identifying the elements that are constant, those that change, and those that constantly change. An example is rate setting in banks – large frauds such as the 2012 LIBOR scandal or the 2013 Forex scandal could have been detected, and further propagation contained. The indications of cartelization, and information bigotry evident in both these scandals could have been detected with this vital triad. Instead, the scandals were detected (LIBOR in 2012 and Forex in 2013), several decades into their making, severely impairing the chances of restitution for the affected parties. In fact, the affected parties may never claim compensation, even if restitution was possible.

Developing Foresight with Analytics and Machine Learning

Bank economists use trend impact analysis to extend their view into the future; as in, what we see today, will grow to a bigger number in five to ten to fifteen years if the conditions supporting it persist. A clear example of this is the 72-year Bull Run3 in US property prices. A view of the future, complemented by analytics and machine learning, could have helped detect the 2008 credit crisis, years earlier. This is not to discount the impact of public policy firing up the sub-prime market; on the other hand, the use of these tools would have enabled timely detection of the underlying process gaps and malicious intent to instigate a reversal of policy.

Fraud detection has shifted to continuous, real-time monitoring of operations and infrastructure use to identify anomalous behavior from the traditional methods of performing audit checks (which typically happen in silos) and connecting them to financial statement mismatches. Fraud prevention techniques and tools need capabilities to anticipate and prevent the ‘unknown’, which can be achieved by collecting horizon data, parts of which may initially seem irrelevant to banks. Mapping such data to transactions and configurational and operational data will help derive new possible scenarios for the current business environment and internal control factors (BEICF).

Statistical techniques such as Bayesian networks will yield valuable insights into possible and probable fraud scenarios. This apart, feeding the data to possible internal scenarios and determining their probability of occurrence given the bank's BEICF, is an important exercise. Horizon scanning data will therefore help internalize possible fraud scenarios that were previously not on the bank's radar because of their failure to perform the mapping exercise and recognize such scenarios. Regular mapping of horizon data to internal data will help the bank shift from a fraud-detection mode to a fraud prevention mode.

Developing machine learning algorithms relevant to the scenarios or combinations thereof, and validating them with relevant data sets will enable the automation of the fraud prevention and early warning systems. The strength of such an approach stems from the fact that it will span business, operations, and technology domains. The algorithms must be validated in context by subject matter experts for relevance to enable banks to choose the right predictors and their correlations. The non-occurrence of these scenarios is the desired outcome for fraud prevention.

Thereafter, when new horizon scan data is received, the scenarios and their random combinations are parsed to predict fraud. When alerts are received from the early warning system, appropriate changes must be triggered in the existing BEICF to prevent fraud. The system 'learns' with every new set of data and matures in 'intelligence'.

Putting the 'Vital Triad' to Work

Horizon scanning is an efficient way to collect data from across enterprises using similar architectures, services or business models. This technique helps bridge data deficiencies for scenario development and validation by leveraging the learnings of the entire ecosystem to create exponential value for the banks. New data sets that hitherto appeared irrelevant to the bank, may prove valuable in new scenario or context development. Cloud technology aids collating and analyzing large data sets for business use at affordable cost of use and maintenance – coupled with analytics and machine learning, this can facilitate the development of an intelligent and data driven approach to fraud prevention. Such an approach will enable banks to proactively adopt disruptive technology innovations without fears about fraud emanating from their systems, processes, and workforce. Given all these advantages, banks must actively consider leveraging the vital triad of horizon scanning, analytics, and machine learning to develop a futuristic approach to fraud prevention in an era characterized by disruptive technologies and business models.

About The Author

Dr. Uma M Somayajula

Dr. Uma M Somayajula is a domain consultant with the Risk Management Practice of TCS' Banking, Financial Services, and Insurance (BFSI) business unit. She has more than 15 years of experience in strategy consulting and developing IT solutions for enterprise risk and security management. Somayajula's current areas of interest include applying analytics in risk management, machine learning and design of futuristic operational risk management techniques for banking and financial institutions.

Sowmyanarayanan VJ (Sowmy)

Sowmyanarayanan VJ (Sowmy) is a consulting partner with TCS' Banking, Financial Services, and Insurance (BFSI) business unit. He specializes in operational risk management, and is a subject matter expert in matters related to policy, risk appetite, insurance, risk technology, and enforcement actions across the areas of treasury, capital markets, and investment banking. Sowmy has been instrumental in the development of offerings and operationalizing risk & compliance services at Deloitte, KPMG, and other large consulting firms. He engages with startups as part of TCS' co-innovation program to develop risk service offerings for global financial firms.

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 09 I 18