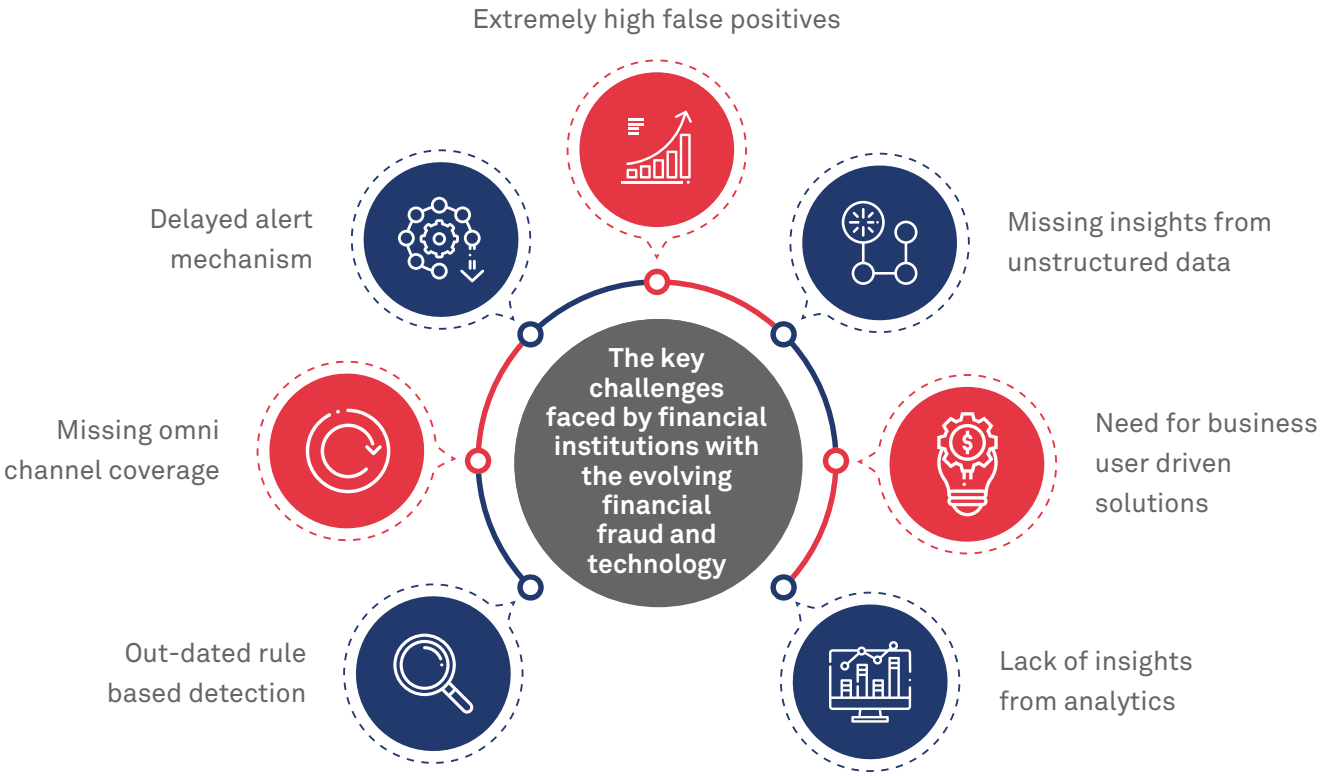
Fraud detection and prevention

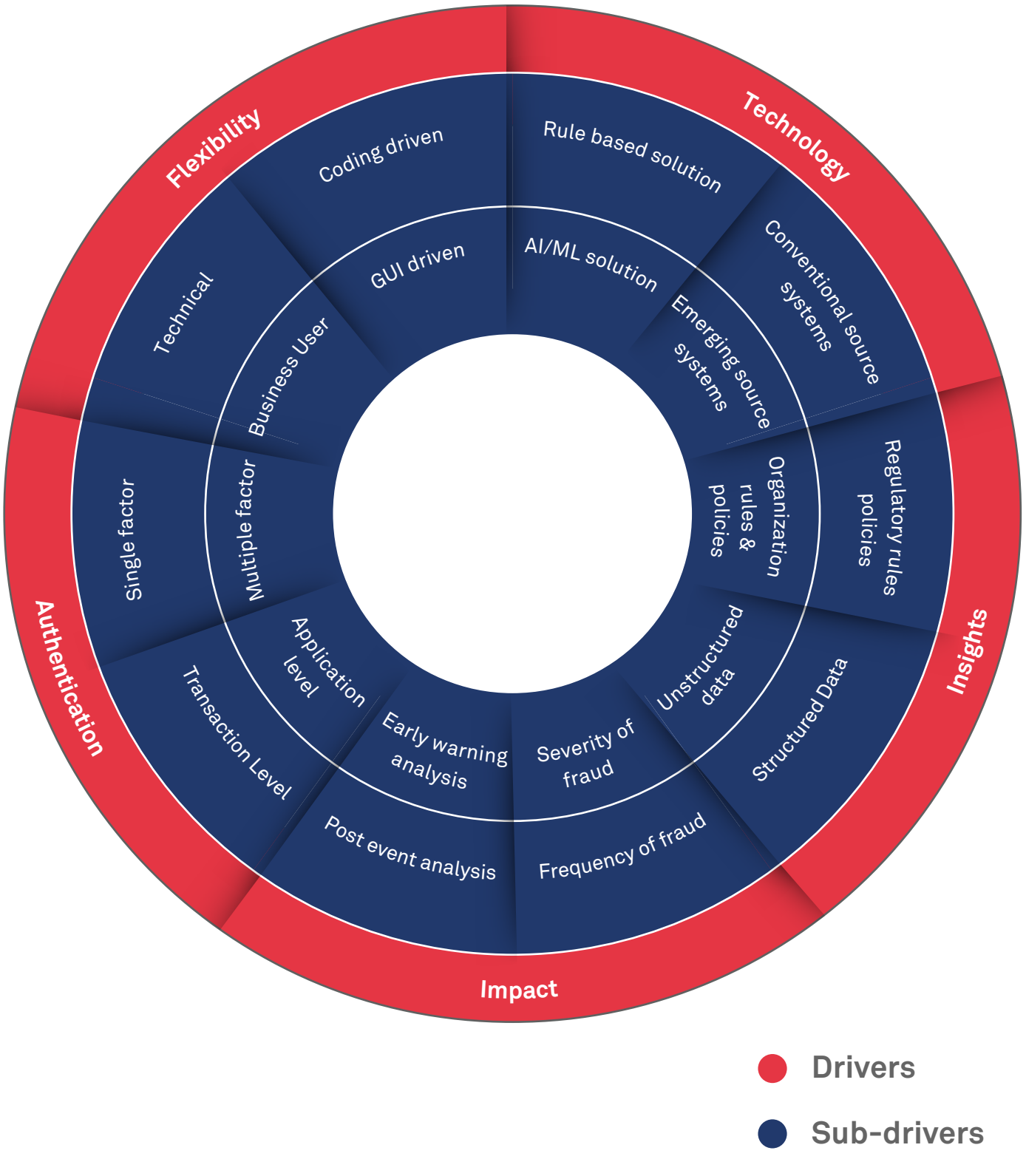
The regulatory compliance of financial institutions is growing at a faster pace than before. Moreover, technology firms are reciprocating with solutions at an even higher pace. Of late, emerging technologies like artificial intelligence and machine learning have seen practical applications, which were earlier restricted to theory. Multiple specialized and boutique firms are now offering domain specific solutions and use cases against the big players who use artificial intelligence and machine learning as a platform.

Institutions facing losses from financial crimes are growing at a similar pace. Fraudsters keep innovating and beating the system. This calls for a solution where technological advancements have to be leveraged to beat the fraudster and allow early identification of their modus operandi.

The following details the key challenges faced by institutions in detecting financial frauds.



The following **five drivers, sub-drivers** and **trends** are redefining fraud detection and prevention requirements of financial institutions. With evolving technology, financial institutions are rethinking their organizations strategy to control internal and external fraud – in both offline and real-time modes.



The following **technology (driver)** matrix indicates the market potential and trends for **fraud detection systems** (Rule based systems, AI/ML technology) against the **Source systems** (conventional source systems, emerging source systems/channels)

Saturated

Rule based - conventional

- Widely present in the market and highly saturated to the point of replacement
- Conventional systems working on typical rule based configurations sending the alerts
- With institutions expecting an upgrade, existing vendors are upgrading their solutions with the latest technology

Rule based - emerging

- Extending the existing conventional solutions to cover the modern and advanced alternate channels like NFC Payments, Wallets, Omin Channel, etc.
- Inability of the solutions to cover alternate channels is pushing companies to reinvent
- Major impact can be seen in the near future as source systems change and last mile connectivity is completely redifining the requirement

Low growth

Medium growth

AI/ML - conventional

- Institutions are pushing for Artificial Intelligence and Machine Learning to bring in operational effieciencies and higher detection ratios with lower false positives
- Deep learning is set to play a critical role in the near future as the rule based system leaves a major areas uncovered
- Institutions that have grown up with rule based solutions are demanding the application of AI/ML to existing processes

AI/ML - emerging

- Dynamic space with inventions at source system layer and detection layers
- Major growth area as new types of frauds with high probability, with lower frequency and increased severity, are expected
- Solution providers are investing in solutions that are in alignment with the roadmap of financial institutions
- Increased adoption of private cloud based solutions

High growth

The following **Insights (driver)** matrix indicates the market potential and trends for **Demanding Authority** (regulatory rules/policies, organizations specific rules/policies) against the **data structure** (structured data, unstructured data).

Saturated

Regulatory - structured

- Highly saturated area where the majority of the institutions are drawing and detecting fraud and insights from structured data, with the common standard rules defined by the regulator
- Once a pattern is detected, rules are defined and maintained as a watchdogs to curtail fraud
- Efforts are made to extend the coverage with new rules using advanced self learning models

Regulatory - unstructured

- Insight from unstructured data has gained prominence over the last two years
- Regulators are pushing institutions to update the risk scores of individuals, entities, directors, etc., based on the insights derived from unstructured data
- Regulators are pushing institutions to consider the insights from social media and unstructured data

Low growth

Medium growth

Organization - structured

- Organizations are moving beyond BAU rule-based to detect the large scale frauds
- Analytics driven alternate measures and rules are being deployed over and above what the regulator defines
- Organizations are inviting experts to compete amongst themselves to identify fraud patterns in organizations

Organization - unstructured

- Institutions are demanding that solutions providers make compatible to derive insights from unstructured data from live streams/feeds, news, libraries from social media, etc.
- Institutions are proactively taking steps to adhere with regulations, which helps with a reduction in NPA's & early fraud detection
- A high growth area in the near future

High growth

The following **impact (driver)** matrix indicates the market potential and trends for the **quantum of fraud** (Frequency of fraud, severity of fraud) against the **timing** (post-event analysis, early warning analysis).

Low growth

Frequency - post event

- Highly saturated BAU process where organizations have stabilized themselves enough to identify the post-event detection
- What is eye-opening is the frequency of post-event detection, from months to days, and days to daily
- Real time and near real time fraud detection is taking centre stage, especially on transaction monitoring

Frequency - early-warning

- Increased interest and adoption of algorithms is promoted by organizations for early detection, prevention and frequecny of fraud
- Highly promoted and applied to corporate and high value loans to prevent fraud and decrease the probability of NPA's

Medium growth

Medium growth

Severity - post event

- Major shifts and indications is seen across signs of low frequency - high severity fraud and losses
- This has a huge reputational risk and imapct on organizational stability
- Proactive measures, learning from establishments of centralized dedicated units under regulators, with the sole purpose of sharing selected data amongst peers in the interests of the group, is gaining prominence

Severity - early warning

- Highly dynamic area and the area to watch out for over the next decade
- Adoption of advanced tools, deployment of complex measures and algorithms, covering the extremes of data for early detection and prevention of fraud
- The coverage includes each and every activity which may question the stability of the institution itself

High growth

The following **authentication (driver)** matrix indicates market potential and trends for the **level of authentication** (transaction level, application level) against the **stages of authentication** (single factor, multiple factor)

Saturated

Transaction - single authentication

- Purely transaction focused and widely used to minimize basic fraud
- Majority of the institutions are compliant as this is a regulatory norm and basically expected from the customer
- No major developments expected, as this has matured without much difficulty

Transaction - multiple authentication

- The rapidly changing eco-system around transactions, and loop holes beyond the single factor authentication has encouraged multi-factor authentication
- Institutions are callingfor multi-factor authentication solutions to complement the core fraud detection framework, to allow end to end control over transactions
- The rise of alternate and omni-channels have paved the way for multi-factor authentication which includes OTP, security grids, challenge questions, etc., that go beyond basic login credentials

Medium growth

Low growth

Application - single authentication

- The growth of omni-channels and alternate channels have pushed for the adoption of application level authentication
- While the transactions were getting authenticated with basic credentials, increased frauds were being detected, with stolen basic credentials emanating from fraudsters via media
- This needed the basic application to be authenticated, within the device being utilized like laptops, mobiles and tablets

Application - multiple authentication

- High growth area and maximum innovation and investments made by organizations to reduce the layers of authetication
- Emergence of risk based authentication solutions which almost nullify frauds of high frequency and volume
- The strongest layer outside the core fraud framework is to block the fraudster from entering the banking system for any activity
- The inclusion of device level authentication which covers and risk scores the considering the parameters of transactions, applications, device profiling, IP addresses, KYC data, etc.

High growth

The following **flexibility (driver)** matrix indicates the market potential and trends for the **user type** (technical user, business user) against **solution usage** (Coding, GUI driven)

Low growth

Technical user - coding

- Solutions with heavy dependecy on coding and black-boxes are going to die
- While coding can be restricted to minimal usage, and as long as it doesn't become a road block to business users, adoption will continue
- Institutions want coding to be owned by the solutions providers, reducing the dependency of in-house technical personnel to BAU only

Business user - coding

- Business users which covers and risk scores the considering to provide insights with decision makers getting centre stage
- Solutions which demand technical know-how and coding, to support the business user's decisions, will be thrashed from the market

Medium growth

Saturated

Technical user - GUI

- Organizations are investing in solutions which will simply do the work
- GUI driven solutions and development is a trend which is appreciated by technical users
- Consoles and frameworks simplify the turn around time for deployment of highly complex development and
- Watch out for developments in the area of integration, for real time detection

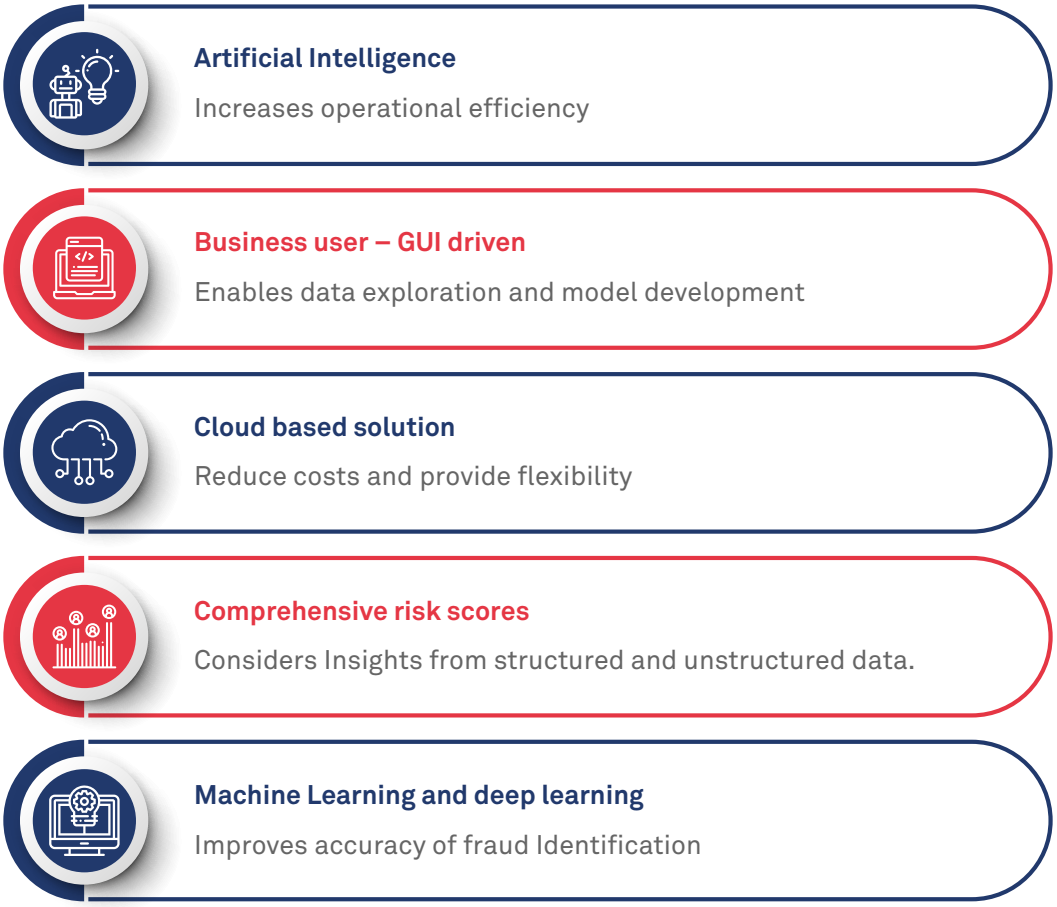
Business user - GUI

- Highly sought after, as this empowers business users with insights
- Faster decision making in data discovery platforms and what-if analysis
- Solution providers are investing heavily, to impress business users with GUI driven and user friendly solutions

High growth

The next decade will experience a transformational shift in the areas of fraud detection and prevention as institutions look out for solutions which provide transformational benefits and ROI.

Benefits and ROI



Getting applied to

Early detection and prevention of high severity as a top priority

Real-time curtailing of business as usual

Financial crime detection and prevention is critical in any organization. Augmenting it with Artificial Intelligence and Machine Learning goes to show how far the industry has come in both theory and implementation.

About the author

Sharad Kumar Ragam
Practice Manager for
Financial Risk & Compliance
Wipro Ltd.

He has 11+ years of implementation, consulting and solutions experience, addressing the banking customers' needs across Fraud Risk Management, Basel & Regulatory Guidelines and Integrated Risk Management.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/BRD/SEP 2018-AUG 2019