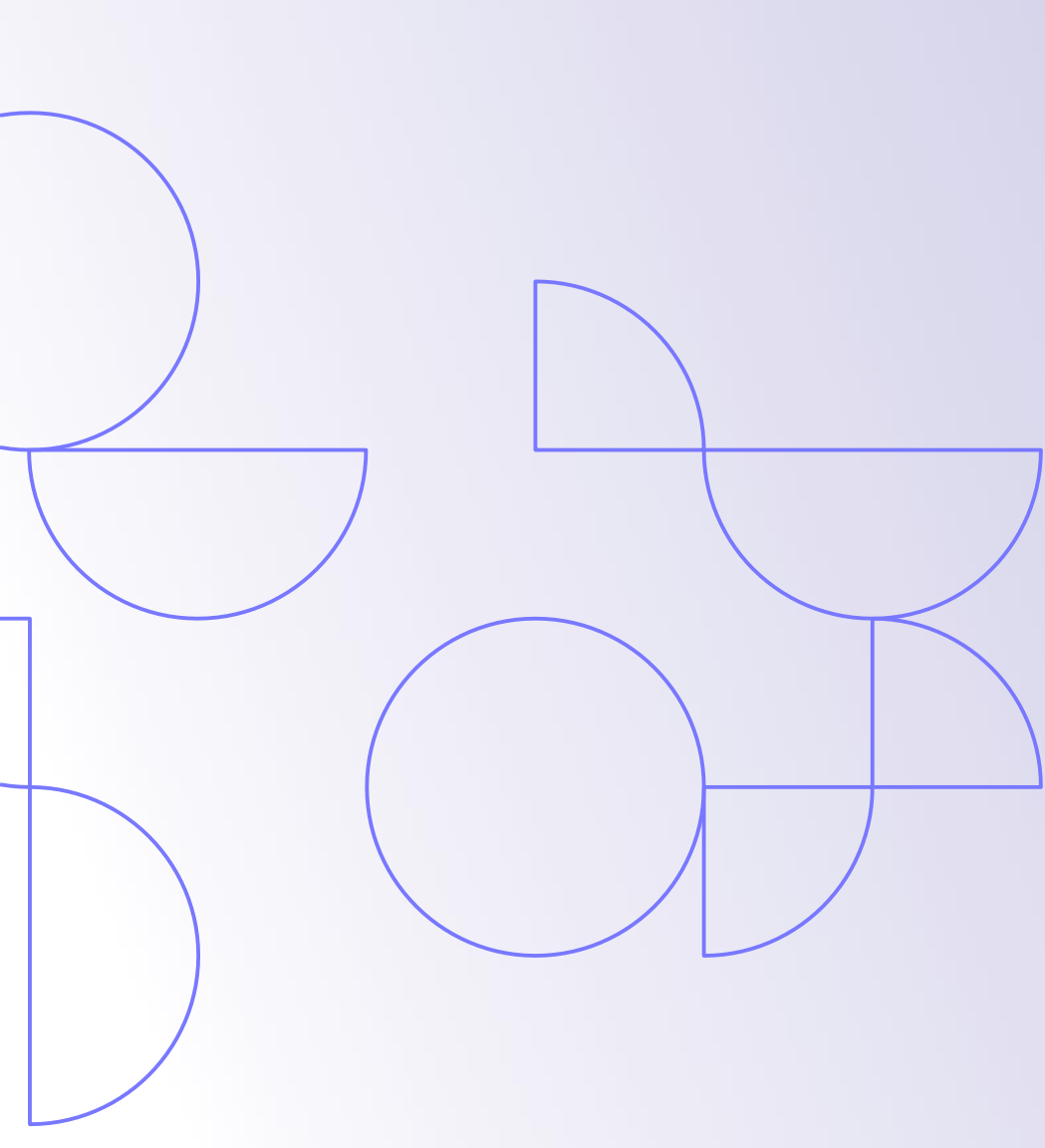


Machine Learning

Predictive analytics and deep learning to detect evolving financial crime



Bad actors are constantly exploring new methods and technology, including artificial intelligence (AI), to devise financial crime attacks.

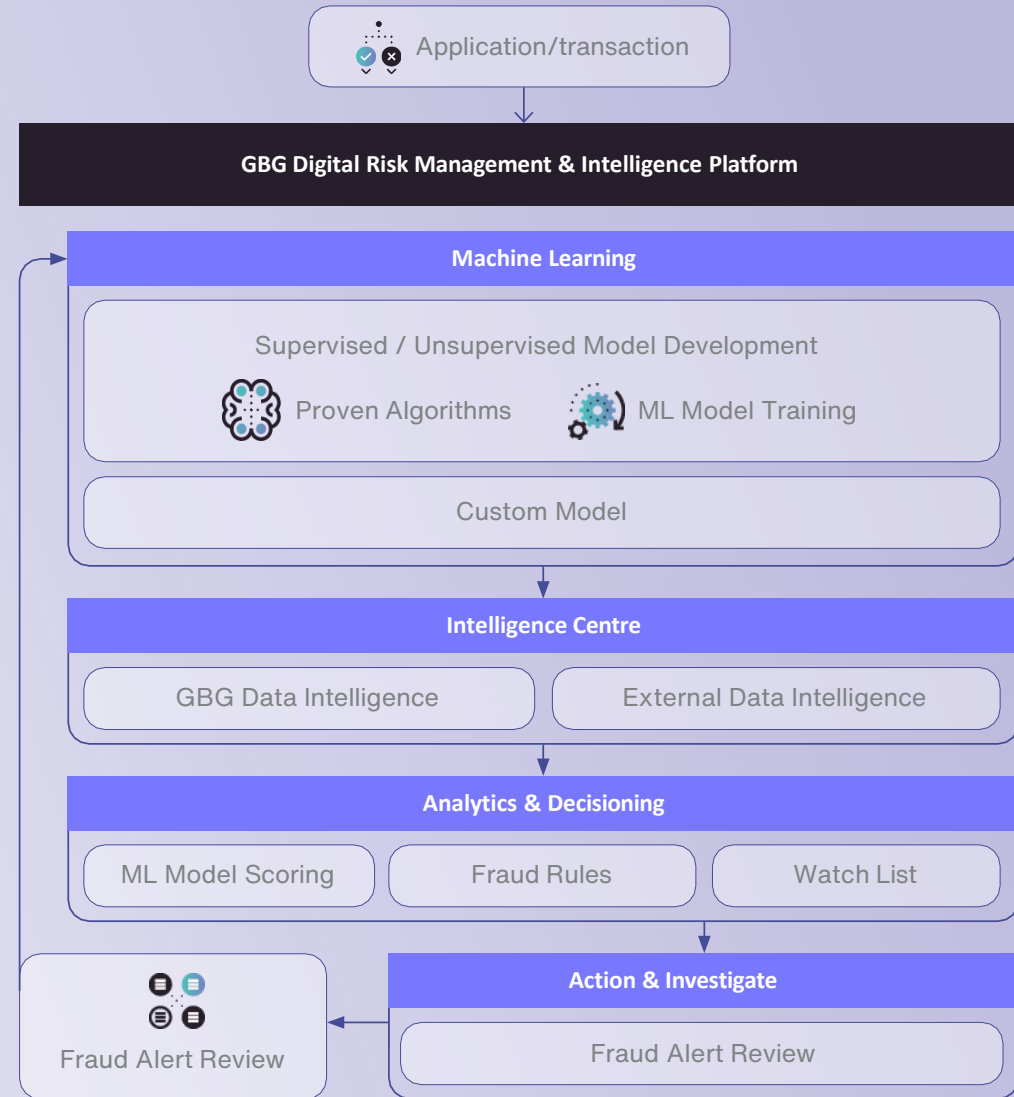
Fraud management that relies exclusively on rule-based, conventionally programmed systems and manual evaluation to detect financial fraud no longer provides adequate defence. With new fraud patterns rapidly evolving, traditional rule-based systems are unable to keep up, resulting in too many false positives, false negatives or allowing frauds to go undetected – resulting in huge financial losses.

Machine Learning uses high performing algorithms for fraud detection, such as neural networks, random forests and gradient boosting machines, to analyse and learn from past actions and behaviors for enhancing fraud detection accuracy and reducing false positives.

Through deep learning, data with known actions and outcomes is used to automate the training of models to detect complex financial crimes that have not been identified by traditional detection approaches such as business defined rules. The added layer of intelligence improves fraud detection rates, increases operational efficiency and supports a larger volume processing, by predicting fraud patterns and recommending new detection parameters for more accurate risk assessment.

Protect your business and customers from evolving financial crimes during the onboarding and transaction:

- Deploy leading edge Machine Learning model deployment for intelligent fraud detection.
- Automate learning to stay on top of evolving fraudulent behaviour patterns.
- Harness the benefit of artificial intelligence with domain expertise and insights.
- Reduce of false positives to focus investigation effort.



KEY BENEFITS

Deploy Machine Learning with leading edge algorithms for fraud detection



✓ Open, user controlled interface enables building, training and throttling of score threshold based on the organisation's fraud risk appetite and alert management capacity.

✓ Keeps a log of all testing, audit and changes made.

✓ Transparency in modelling parameters to support regulatory compliance requirement.

✓ Contributing features to fraud results are displayed to the investigator along with the score to provide model transparency compliance.

✓ Intuitive user interface to drill down into output and data.

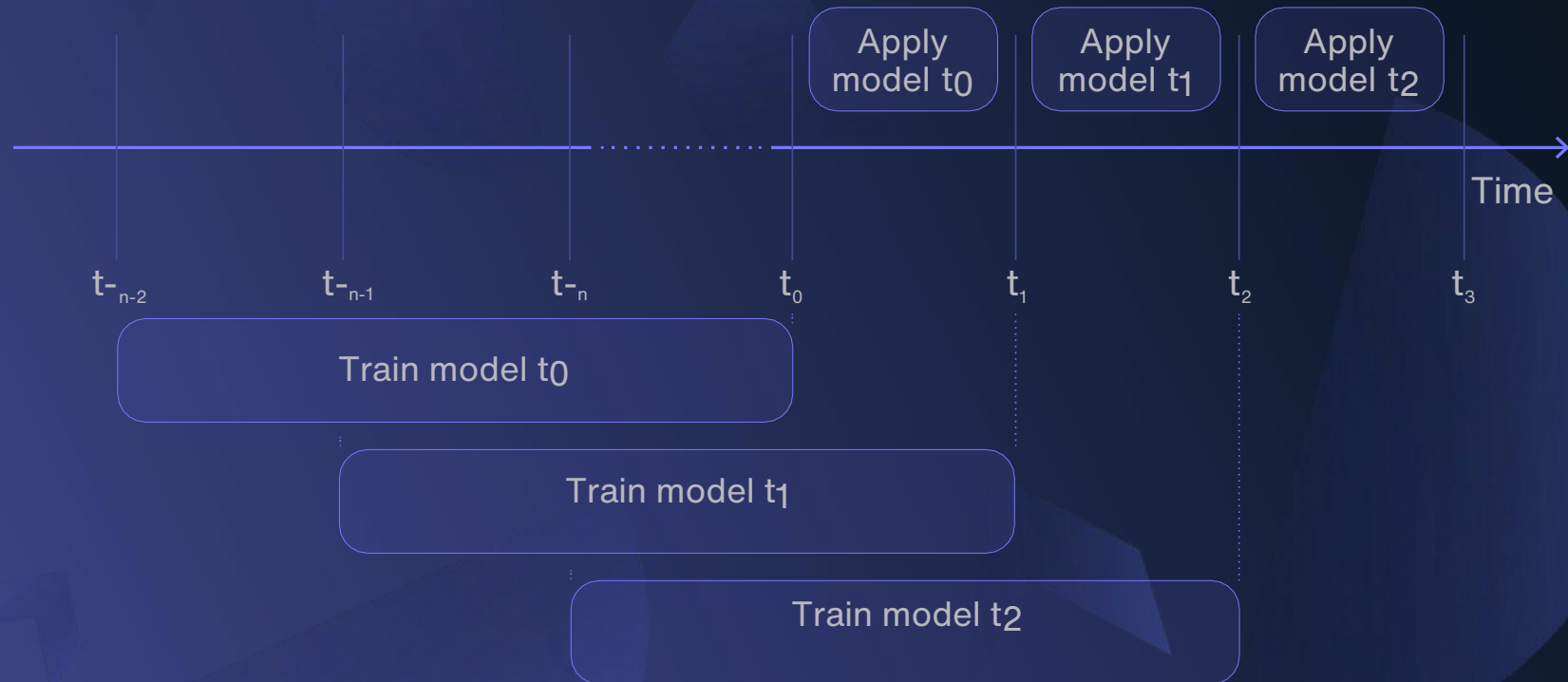
✓ Custom model development is available as a GBG service.

KEY BENEFITS

Automated learning to stay on top of evolving fraudulent behaviour patterns

Continual and autonomous model training to mitigate the issue of model deterioration.

Adopts dynamic sliding window approach to retrain a classifier everyday on new supervised fraud cases.

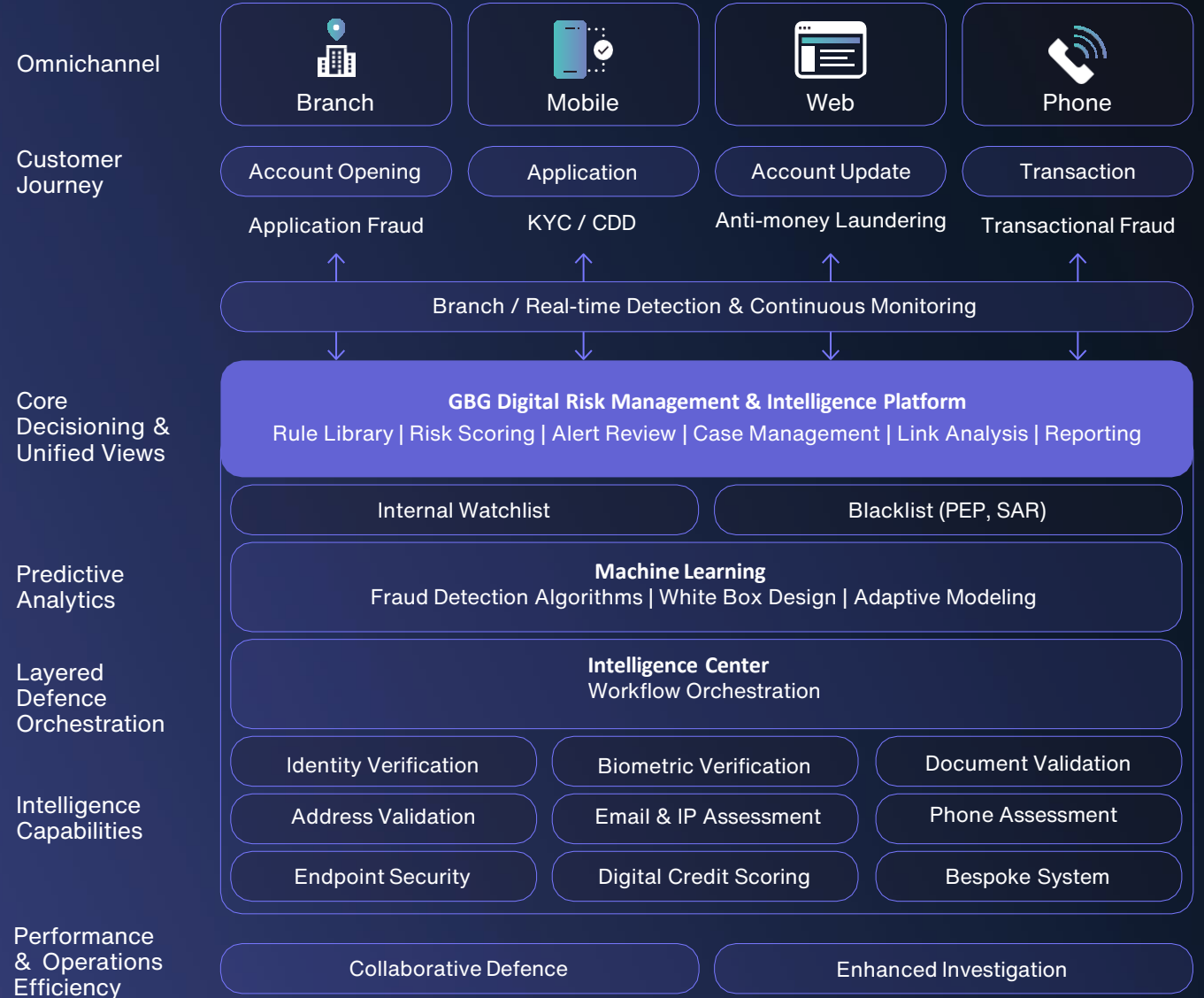


KEY BENEFITS

Augment fraud detection with additional data sources from GBG and third-party

More data improves the machine learning model, as data richness enables differences and similarities between multiple behaviours to be picked out. With more data sets available, it provides correlation view of what is genuine and what is fraudulent.

Machine Learning has the ability to augment fraud detection by calling in data on behavioural, biometric, attributed and digital identity of the individual, as well as online and cyber footprint.



Using advanced analytics to detect more fraud

Challenges

- Increasing number of review alerts with growing number of applications being processed. Using manual review processes to manage the increasing number of alerts will result in additional workload and operational cost for fraud team.
- Unaddressed gaps in existing detection processes will result in additional financial loss from fraud.
- Limited amount of training data can make it difficult to identify patterns or variables to use as rules.

How Machine Learning Can Help

A tier one global bank detected 25% more frauds with Machine Learning

Advanced Analytics Fraud

Use advanced analytics to uncover more fraud, with a lower alert trigger rate.

Uncover Hidden Fraud

Detect hidden fraud using data that legacy software has missed.

Enhance Models with Data

Apply third party data to enrich detection models.

Maximize Fraud Tech ROI

Improve the returns on fraud investigation technology investment.

Minimize Investigator Workload

Reduce workload for investigators.

Enhance Investigation Productivity

Optimise investigation efficiency.

KEY BENEFITS

Improve fraud detection precision



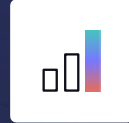
Identify more fraud

Identify more fraud without an increase in review alerts.



Predictive analytic models

Capture sophisticated fraud using advanced predictive analytic models.



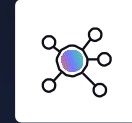
Increased ROI

Get better return on investment on financial crime prevention expense.



Faster onboarding

Speed up onboarding for good customers.



Better customer experience

Enable a frictionless customer experience.

Prevent more fraud at the point of onboarding with improved fraud detection rates

Challenges

- Third party fraud is becoming more difficult to detect.
- As bad actors become savvy with fraud detection thresholds and triggers, they are better able to orchestrate attacks that go undetected.
- A growing number of people are victims of fraud due to:
 - Data breaches
 - Account takeover
 - Online scams Malware

How Machine Learning Can Help

Leverage Predictive Modeling

Utilise predictive models to identify new patterns across new and existing applications.

Boost Detection Efficiency

Increase detection rate and efficiency by supplementing predictive detection models with existing fraud detection rules.

KEY BENEFITS

Reduce false positives to enable investigation focus on exception cases



Machine learning

Machine Learning becomes smarter with every application.



Use intelligence

Use intelligence from outcomes of known fraud, missed fraud and high risk behaviour.



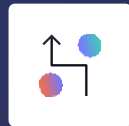
Reduce referrals

Reduce the number of referrals to fraud operations.



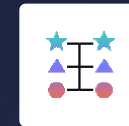
Leverage additional data

Leverage additional data attributes outside of rules for more accurate detection.



Adaptive model learning

Benefit from the automated adaptive model learning based on investigation outcome.



Challenger model

Incorporate challenger model to run in tandem to ensure best detection results.

USE CASE

Reduce alert rates by allowing straight through processing of good customers

Challenges

- An increase in applications creates a greater workload for the fraud review team.
- In an existing system if the number of frauds missed by existing fraud rules are low then it means the detection rules are effective at preventing fraud.
- If there are too many false positives that require manual review additional resource in the application review and fraud investigations team is required.

How Machine Learning Can Help

Streamline Fraud Investigations

Reduce the workload for the fraud review and investigations team

Reduce Alert Volume

Lower the total alert rate for high fraud potential or suspicious alerts within the system

Enhance Fraud Precision

Increase the precision rate with a better ratio of confirmed frauds within the number of alerts for high fraud potential or suspect cases

Combine data intelligence with insights from GBG Fraud and Compliance Expertise

GBG Fraud Specialists and Professional Services Consultants are armed with deep industry knowledge, strong local market insights and operational best practise experience.

Committed to customer success, each solution deployment is a joint-partnership with our client to assess, optimize and deploy fraud detection and compliance solutions, that are fully capable of responding effectively to evolving business needs, protect against online financial crimes and keep to regulatory obligations.

GBG



USE CASE

Uncover suspicious cases in different geographical regions

Fraudulent behaviours are getting surreptitious and can be overlooked as the most nondescript behaviours or attributes. In addition, different geographical regions are seen to exhibit different behavioural tendencies. With artificial intelligence coupled with insights from GBG's fraud expertise, undetected cases can be identified.

On the right are some examples of suspicious cases detected by Machine Learning on GBG Instinct Hub coupled with insights from GBG's fraud specialists.



About GBG

GBG is a global technology specialist in fraud, location and identity data intelligence with offices in 18 locations worldwide.

For over 30 years, GBG has been accessing and verifying identities, to the standards set by financial regulators, of more than 4.4 billion people worldwide or 57% of the world's population. GBG has a network of over 270+ global partnerships and access to 510+ datasets to provide data with accuracy and integrity.

In the fraud category, GBG manages end-to-end fraud and compliance needs across a range of industries including financial services (international, regional and local banks, auto finance companies, P2P lending, mutual companies, and credit unions), government services, retail, betting and wagering. Some of our customers include 90% of top tier banks in Malaysia, BNP Paribas Personal Finance in Spain, regional banks like HSBC, and major wagering players like Tabcorp.

**For more information about
Machine Learning**

contact@gbgplc.com
www.gbgplc.com/apac

GBG Offices Worldwide

APAC: Beijing, Canberra, Jakarta, Kuala Lumpur, Melbourne, Shanghai, Shenzhen, Singapore, Sydney

Rest of World: Barcelona, Dubai, Germany, Turkey, United Kingdom, United States

GBG



Machine Learning

www.gbtplc.com/apac

© Copyright 2021 GB Group plc ('GBG'). All rights reserved.