GBG | Instinct

Orchestration

Layered intelligence for precise financial crime detection

Orchestration for GBG Instinct Hub connects and layers variety of data sources for identity proofing, verification, authentication intelligence on Instinct Hub to strengthen financial crime defence during digital onboarding.

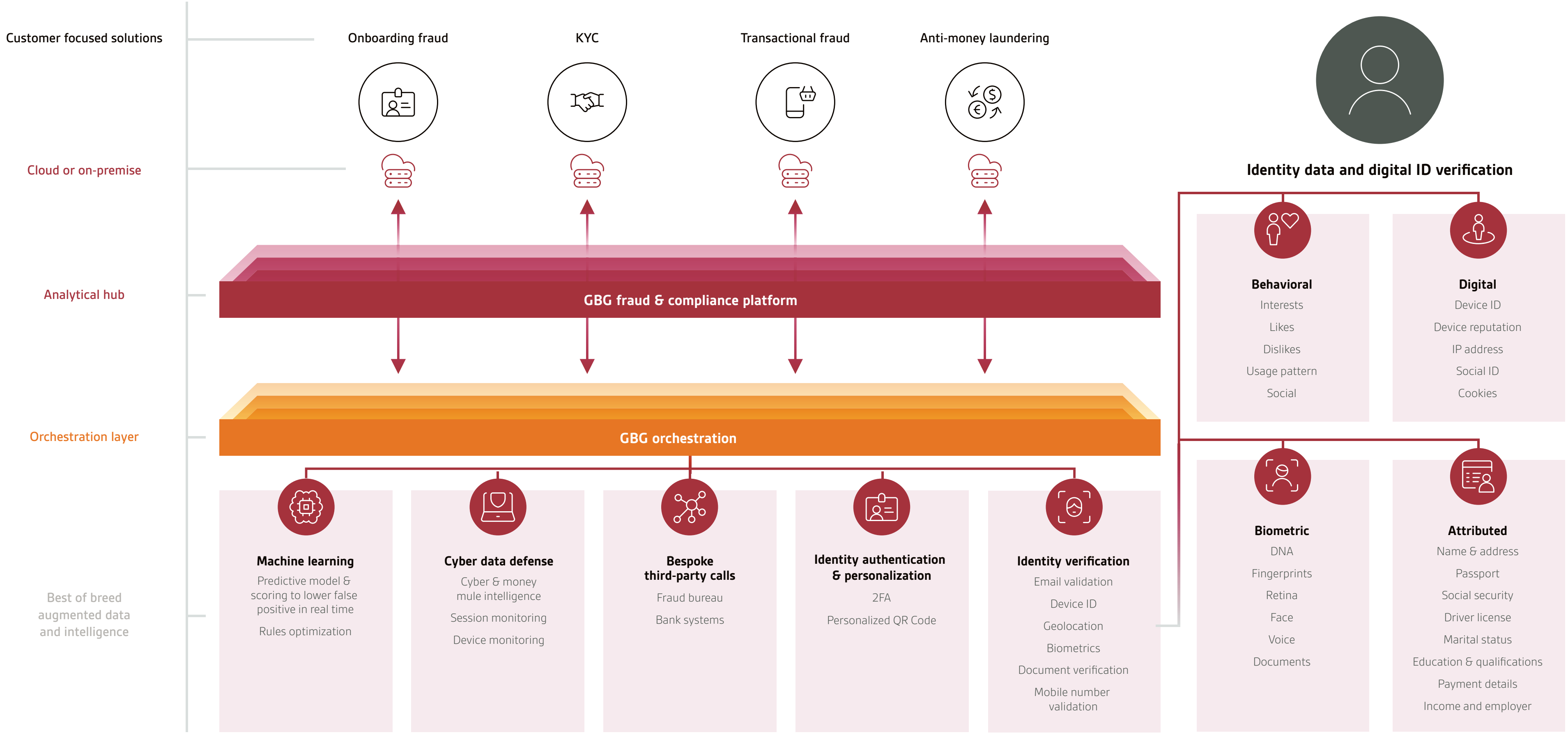
The ability to drill down, expand and co-relate risk identifiers in various profile parameters of a customer proactively increases fraud detection accuracy, especially for online channels.

With its dynamic workflow design, organisations can design the desired fraud check processes to incorporate callouts of multiple data sources, including proprietary data from silo departments as well as external data sources.

Its intelligent data layering allows businesses to automate smart decision making and provide enhanced customer due diligence during new customer onboarding. These capabilities help to enrich each application profile for a comprehensive approach to financial crime control.

Orchestration for GBG Instinct Hub enables layering of different data intelligence for additional fraud and suspicious behavior detection, strengthening financial crime defence against various fraud typologies:

- Synthetic identity fraud
- First party fraud
- Account takeover
- Social engineering
- Money mule crimes
- Money laundering and terrorist financing



Customer focused solutions

Onboarding fraud

KYC

Transactional fraud

Anti-money laundering

Cloud or on-premise

Analytical hub

GBG fraud & compliance platform

Orchestration layer

GBG orchestration

Best of breed augmented data and intelligence

Machine learning
Predictive model & scoring to lower false positive in real time
Rules optimization

Cyber data defense
Cyber & money mule intelligence
Session monitoring
Device monitoring

Bespoke third-party calls
Fraud bureau
Bank systems

Identity authentication & personalization
2FA
Personalized QR Code

Identity verification
Email validation
Device ID
Geolocation
Biometrics
Document verification
Mobile number validation

Identity data and digital ID verification

Behavioral
Interests
Likes
Dislikes
Usage pattern
Social

Digital
Device ID
Device reputation
IP address
Social ID
Cookies

Biometric
DNA
Fingerprints
Retina
Face
Voice
Documents

Attributed
Name & address
Passport
Social security
Driver license
Marital status
Education & qualifications
Payment details
Income and employer

Key Benefit

Protect your organisation against existing and new advanced online and cyber end-point threats

- Connect to preferred proprietary or desired external data source
- Create workflows to automate even the most complicated financial crime detection process
- Design and modify onboarding workflow easily with drag and drop workflow builder and inbuilt data connectors
- Reconfigure rules, workflows and data sources with a single click
- Fast adaptation to changing regulatory requirements for Know Your Customer, Anti-Money Laundering and Counter-Terrorism Financing
- Respond quickly to evolving financial crime landscape and help save business from losses and investigation cost

Use Case

Orchestrate a multi-layered defense against account takeover

Challenges

- Data silos that exist between different business units, regions or systems within the same organisations
- Finding meaning in massive amount of data from third-party sources with different data formatting and naming conventions

How Orchestration Can Help

Orchestration layers information from various data sources to identify unusual behaviour that could be indicative of account take over. For example:

- Activity from a new user device
- The absence or presence of malicious software
- The absence or presence of connection to other actions associated with the account
- A large value withdrawal or transaction inconsistent with customer profile

Key Benefit

Activate and access best of breed fraud detection solutions easily

- Integrate the required solutions into your fraud detection platform to respond to new digital fraud attacks swiftly:
  - Machine learning
  - Cyber data intelligence
  - Identity and geolocation verification
  - Identity authentication
  - Bespoke third-party calls to fraud consortiums and proprietary banking systems
- Enhanced fraud checks on the e-DNA of your new customers with email validation, device fingerprint, behavioral patterns, personal documents, geolocation and blacklists
- Leverage on historical behavior and transactions to validate the authenticity of your new customer
- Connect to fraud consortium data or proprietary data to augment data sources

Use Case

Enable device fingerprinting, geolocation and identity checks to protect against account takeover and cyber enabled fraud typologies

Challenges

- The growing number of data breaches means that more individuals are at risk of identity theft
- Bad actors learn quickly and can engineer attacks to work around the safeguards in an organisation's defense program
- Programs are leveraged to swiftly gain access on stolen identities, while virtual machines and emulators are used to simulate mobile devices
- Difficulty in configuring and integrating new validation sources to existing systems.
- Static workflows are unable to accommodate special cases or customer specific detection handling techniques

How Orchestration Can Help

- GBG Orchestration layers information from various data sources to facilitate monitoring of a web or mobile session, to detect unusual device or end user behavioural patterns, which maybe an indication that the account has been hijacked:
  - Physical and online transactions time zone anomalies
  - Conflicting omnichannel usage
  - Mobile device operating system changes
  - User profile language change
  - Presence of malicious software
  - Connection to other actions associated with the account
  - A large value withdrawal or transaction inconsistent with customer profile
  - Compare user's mouse movements, keystrokes, typing cadence, delays and navigation velocity to that of the authentic customer
- Incorporate diverse insights and dynamic processes across a range of third-party crime prevention solutions to ensure businesses have the best defense against fraudsters

Key Benefit

Increase fraud check accuracy by up to 30%*

- GBG Orchestration automates the detection of suspicious behaviour on the individual and the co-relationships surrounding the individual
- Users have the ability to customise the fraud detection workflow to better suit individual business needs
- Fraud investigators are able to drill down into data to make faster informed decisions

*Based on customer beta test results

Use Case

Manage risk within high value product application assessment

Challenges

- Creating appropriate experiences for each individual and for each financial product
- Ability to customize the fraud detection workflow to better suit the business needs
- Detect and prevent all types of fraud:
    - First party fraud
    - Syndicate fraud
    - Account takeover

How Orchestration Can Help

- Identify intricate fraud attacks by using decision models that create risk profiles based on correlated variables
- Process applications quickly and with confidence by using predictive models to make decisions
- Set inbuilt workflows to segment applications based on the initial risk score to ensure proper due diligence process is followed and further verification is sought as appropriate
- Move good customers through the system quickly with the option to layer in additional data point verification as required
- Automate more application processing with enriched rules-based approval to free up resource for exception 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.

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 GBG Instinct Hub

E: contact@gbgplc.com
W: 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 | Instinct

www.gbgplc.com/apac