



GBG | Instinct  
Intelligence Center

Orchestrate layered defence  
against evolving financial crimes



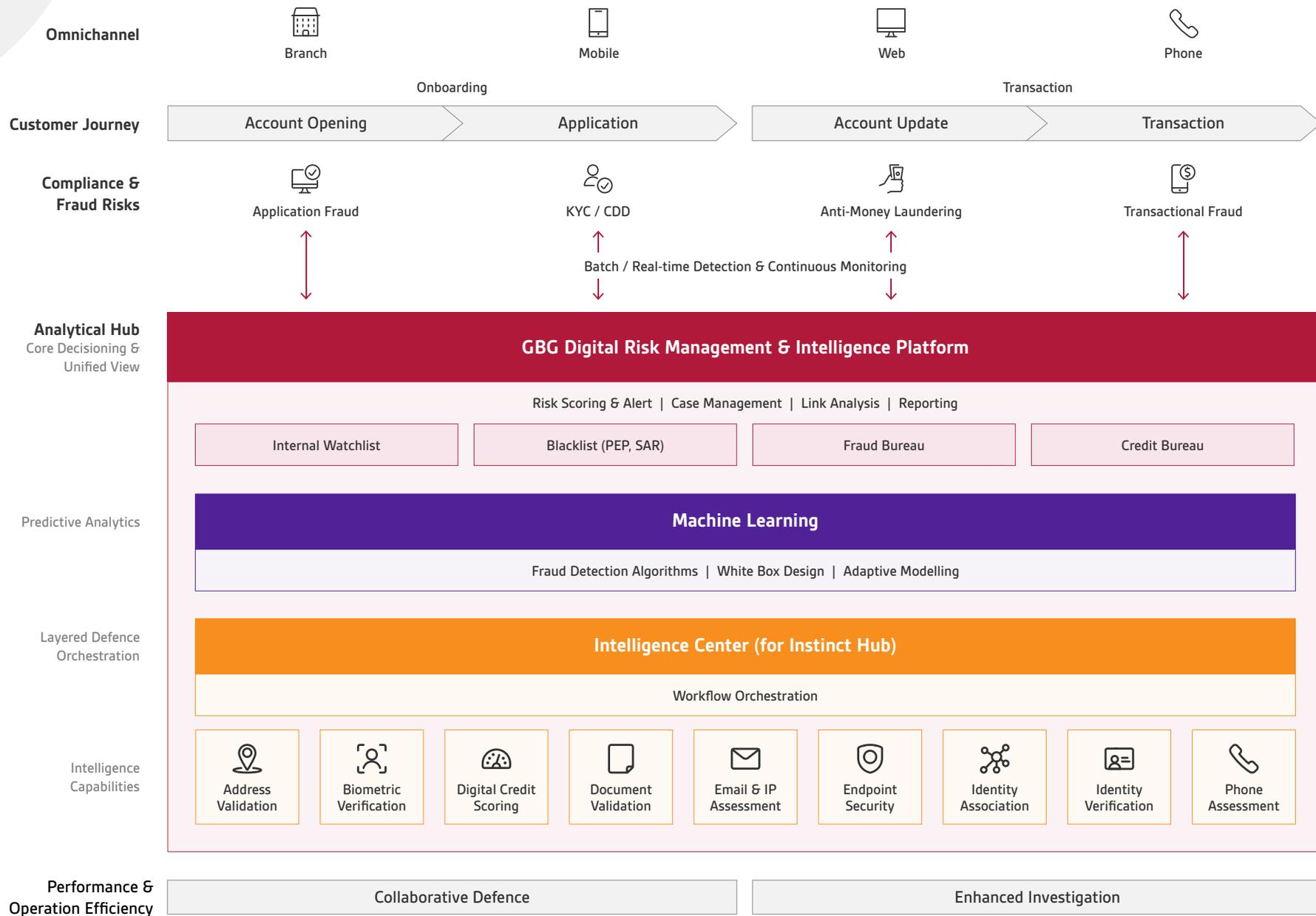
**Accelerated digital adoption is making the digital space attractive for criminal activities. Businesses need to stay vigilant in keeping their defence with up to date solutions to respond effectively.**

The Intelligence Center for Instinct Hub enables organisations to stay agile with access to advanced capabilities and data intelligence, to protect themselves and their customers against evolving financial criminal behaviours during the onboarding and application process.

With Intelligence Center, fraud risk managers can orchestrate and design the desired fraud assessment processes using its workflow manager, leveraging advanced intelligence capabilities such as email, Internet Protocol (IP) address and phone risk assessment, endpoint security and digital credit scoring. The outcome is an enriched insight on fraudulent applications based on the alternative risk indicators for more accurate assessment and reduced false-positive instances.

The Intelligence Center offers access to a comprehensive range of best-in-class fraud risk assessment capabilities from GBG and our choiced partners to enable strong layered financial crime defence against fraud typologies such as:

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





## Protect your organisation and customers from complex financial crimes

- Design effective fraud solution workflow by orchestrating different intelligence capabilities
- Modify workflow easily for adapting to changing AML/KYC regulatory requirements and evolving financial crimes
- Consolidate view of fraud risk triggers with intelligence derived from the different capabilities, rules and watch lists
- Drill into each risk indicators for insights on cybercrime tactics and behavioural patterns to facilitate investigation and improve future solution design

## Use Case

# Orchestrate a multi-layered defence against account takeover

### Challenges

- Limited, silo data and detached, purpose-specific solutions are single dimensional and fragmented
- Difficulty in correlating data and intelligence from multiple different sources for meaningful insights
- Potential loopholes for fraudulent attempts to go undetected

### How Intelligence Center Can Help

Intelligence Center enables orchestrated detection and aggregated intelligence to identify indistinctive behaviours that could be indicative of account takeover:

- Activity from a new or blacklisted device
- Presence of malicious software on device
- Use of a new or inactive email or mobile account
- Application or transaction behaviour inconsistent with the customer profile, such as an unusually large or increased value in application or transaction



## Keep fraud solutions current with best-in-class intelligence capabilities

- Benefit from a dynamic library of proven intelligence capabilities for fraud risk assessment, collated from within GBG and our partners, based on our decades of fraud domain expertise.
- Build strong fraud defence against evolving fraud risks leveraging intelligence capabilities such as:
  - Address validation
  - Biometric and identity verification
  - Document validation
  - Phone, email and IP (Internet Protocol) assessment
  - Endpoint security and authentication
  - Digital credit scoring
- Single interface for quick access and deployment of new intelligence capabilities with minimal downtime

## Use Case

# Effective defence against sophisticated fraud typologies

### Challenges

- Easy criminal access to customer information due to increasing data breach occurrences
- Tech savvy cybercriminals are engineering cyber-attacks, without being detected
- Difficulty in validating origin and legitimacy of application with standard rules and watchlists
- Legacy systems are not designed to accommodate new capabilities or provide consolidated view from multiple intelligence sources
- Slow to adopt new solutions due to stringent procurement process

### How Intelligence Center Can Help

Additional new intelligence capabilities can be activated on Intelligence Center as an integrated solution to help detect suspicious identities, unusual usage or user behavioural patterns during the application process:

- Phone, email and IP assessments detect suspicious indicators on the origin and usage
- Simultaneous or conflicting applications can be detected with address and geolocation validation
- Device behavioural patterns enable validation of the device ownership and usage
- Endpoint security authentication further confirms if malicious attempts were made using malware or bot emulator



## **Benefit from GBG's decades of fraud and compliance management expertise**

With operational best practise experience gained from working with top financial institutions and banks around the world, GBG Fraud Specialists and Professional Services Consultants are armed with deep industry knowledge, vital market insights and understanding of the local regulatory requirements.

GBG Professional Services has been consistently delivering effective and proven fraud and compliance solutions to help businesses, from small, mid-sized to large enterprises, be digital-ready without compromising on fraud and compliance risks.

Committed to customer success, each solution deployment is a partnership with our customers to understand the business challenges, identify and assess the requirements, before designing and deploying the best suited solution.

On top of this, GBG Professional Services offers health check, as well as rules and model tuning services to ensure the solutions stay current and continues to deliver consistent and optimal performance.

# 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 Intelligence Center for GBG Instinct Hub**

**E:** [contact@gbgplc.com](mailto:contact@gbgplc.com)

**W:** [www.gbgplc.com/apac](http://www.gbgplc.com/apac)

## **GBG Offices Worldwide**

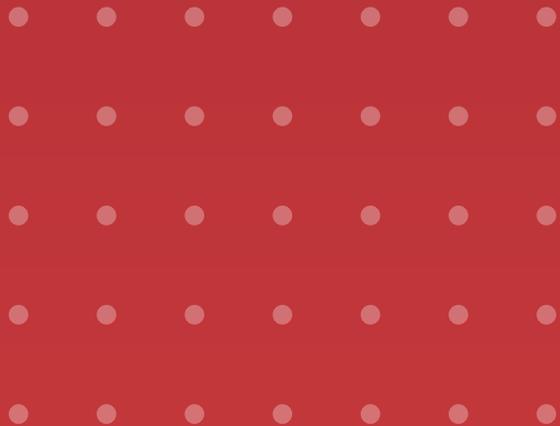
**APAC:** Beijing, Canberra, Jakarta, Kuala Lumpur, Melbourne, Shanghai, Shenzhen, Singapore, Sydney

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



# GBG | Instinct

[www.gbgplc.com/apac](http://www.gbgplc.com/apac)



©2020 GB Group plc ('GBG'). All rights reserved.

Version 09/2020