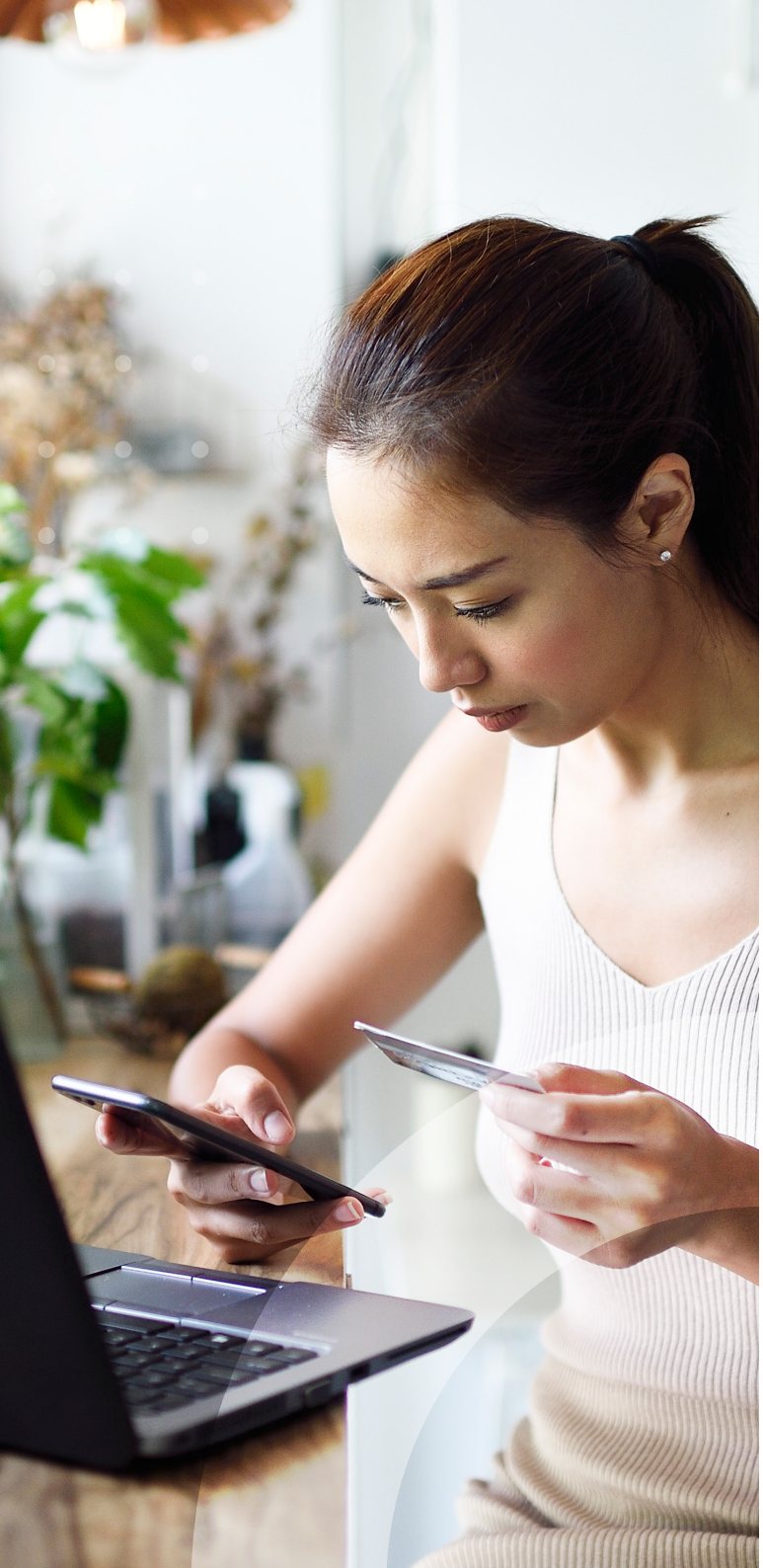
GBG | Predator

Accelerate digital payment and transaction channel growth safely & securely



GBG Predator enables organisations the agility to mitigate fraud and compliance risk for digital payments and transactions across customer interactions.

It is capable of monitoring high transaction volume per second and simultaneously protecting the business against fraud and anti-money laundering. With its intelligent design, fraud specialists can focus on critical information to make faster and better decisions.

Designed for today's fast-evolving digital business landscape, GBG Predator enables organisations to adapt and roll out new online or offline channels quickly, without compromising fraud and compliance risk management requirements.

GBG Predator 5 helps organisations minimise fraud loss and achieve compliance by:

- Enabling real-time decisioning to detect and act on fraud
- Easing new product and channel launch with fraud protection readiness
- Improving productivity and investigator accuracy
- Reducing compliance and operating cost

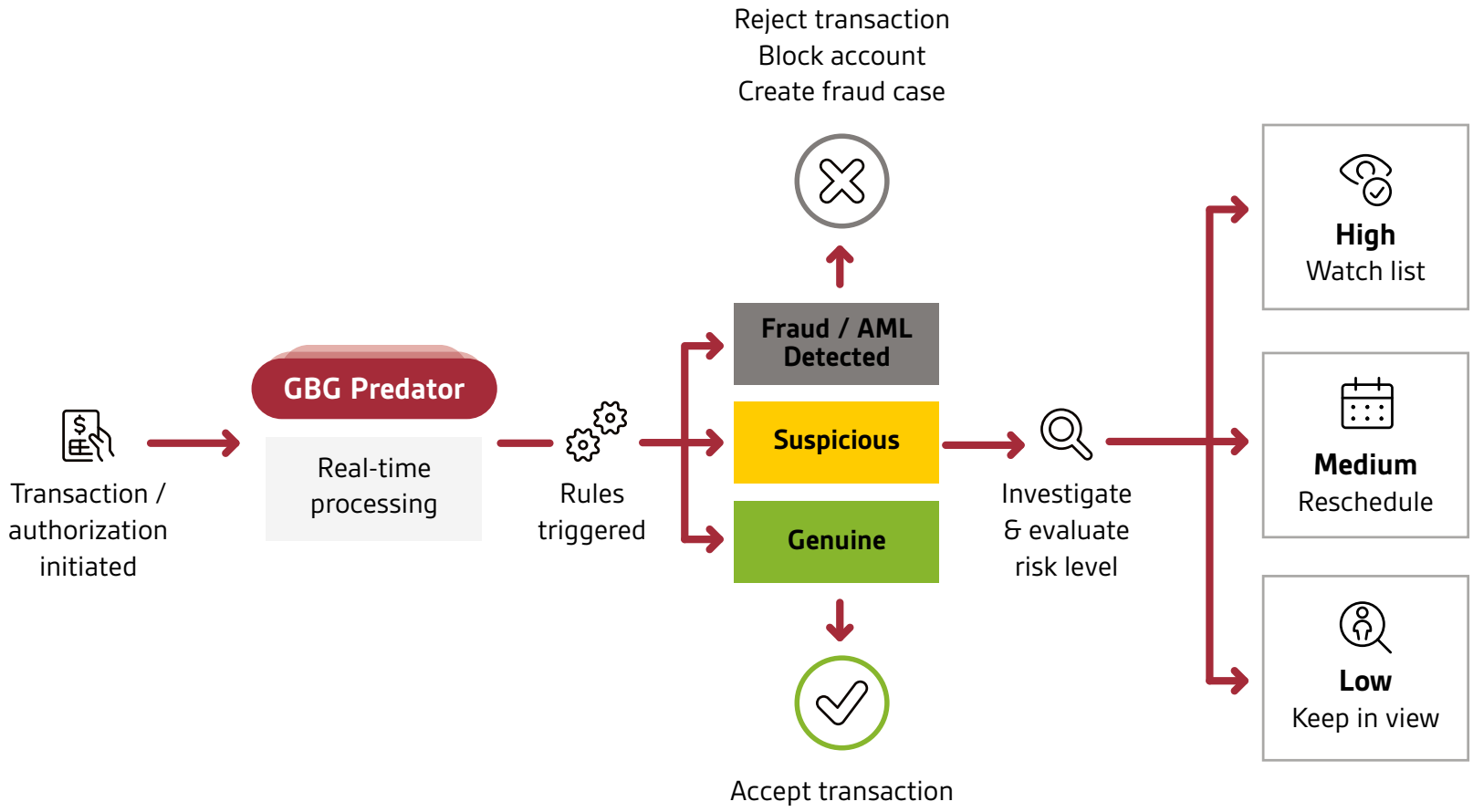
Non-cash transactions will grow and compound by 12.7 % to 2021**

** Global Banking Fraud Survey, KPMG International 2019

Predator 5 protects against modern-day financial crimes including:

- Mule money movement
- Social engineering attack
- Hijack account
- Card not present
- Bots
- Malware
- Payment fraud

GBG Predator Transaction Monitoring



Key Benefit

Ease of launching new products and channels with fraud protection readiness

- Dynamic channel modification enables organisations to quickly and easily add new channels, including ATM, mobile phone, and contactless payment for instant financial crime protection.
- Dynamic behavior modification allows users to add and accommodate new channels, payment types and the associated behaviors flow.
- Ease of integration to respond to customer demands and market changes quickly.
- Quick integration of new data sets with existing information to extract new insights.

Use Case

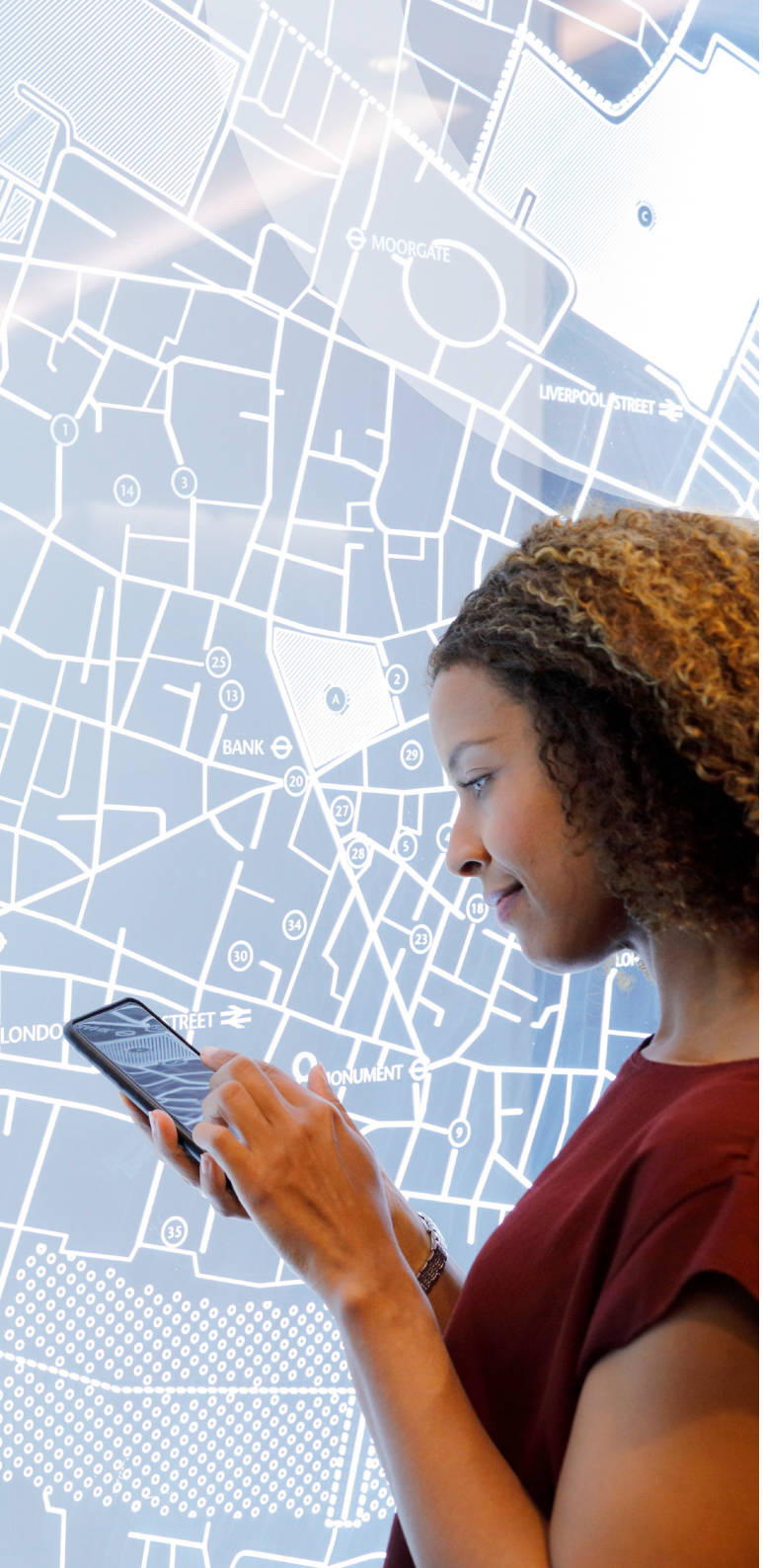
Incorporate data from new channels and partners to build clear behaviour profiles

Challenges

- Incorporating new data channels into an existing system can be a cumbersome technological process which impacts customer experience.
- Consumers demand a fast and seamless transaction experience.
- The payment space is evolving rapidly with the rise of new technologies and vendors to compete with.
- Fraudsters exploits vulnerabilities often present in new services with targeted attacks.

How Predator 5 Can Help

- Add new payment channels for data capturing easily via API.
- Customisable alert screens allow reviewers to filter and focus on meaningful data to make informed decisions.
- Flexible report generation and modification per business requirements.
- Future-ready solution designed to detect financial crimes for both current and new emerging channels.



Key Benefit

Real-time decisioning to detect and act on fraud at the point of origin

- Experience split second decisioning from transaction to customer response.
- Sub-second decision lifecycle to meet requirements threshold expectation for Financial Institutions.
- Identify threats before they compromise legitimate customers and merchants.
- Create intelligent workflows by identifying behavioural pattern baselines and blocking anomalous behaviours.
- Incorporate data from black list, white list and watch list, using one or a combination of the following methods: importing data into Predator, reviewer flagged data for that list, or have Predator's processing algorithm automatically build those lists.

Use Case

Protect clients from threat of account takeover and organisations from financial distress

Challenges

- Fraudsters can gain access to accounts via data theft, malicious software or social engineering.
- Points of failure expose customers to threat can originate from both internal and external of an organisation.
- Client account information and fund becomes accessible upon successful account takeover.
- A fraudster may go unnoticed taking small amounts from a victim's account.

How Predator 5 Can Help

- Identifiy presence of malicious software and unusual device activities.
- Protect users across web and mobile channels, including e-commerce and other third-party platforms.
- Analyse user profiles based on what is happening during the session and how the user behaves (bio-chronometrics).
- By analysing a customer's behaviour patterns, a model can be created to identify unusual activity and send an alert to the customer to verify the transaction.

Key Benefit

Improve and speed up investigation process

- Take a holistic view of a customer, account or entity to make better and faster decisions.
- Inbuilt shortcuts let reviewers triage alerts faster by performing the following actions in one click:
  - Block fraud
  - Mark transactions as genuine or suspicious
  - Add values to a watchlist; for example, account number, merchant number, terminal ID
  - Create or add to a case within the case management system.
- Users can personalise their own review experience by creating new actions, shortcuts, screen views, value lists, insight grids and more.
- Remove unnecessary steps in a process to ensure all relevant transactions and actions are documented for sharing with law enforcement and regulatory bodies.
- Adapt rules and workflows to handle new scenarios easily, without any code change.

Use Case

Keep the most vulnerable members of our community safe

Challenges

- Digitisation of banking services results in a high-level of non-face-to-face service delivery.
- Massive transaction volumes mean each transaction cannot be manually reviewed and could be missed.
- Creative criminals exploit gaps in defence to continually renew schemes to avoid detection.
- Crimes are perpetrated by a person the victim trusts, and the victim may never realise they are being exploited.
- Fake agents, charities and merchants prey on trusting victims and are used to obscure illicit activity.

How Predator 5 Can Help

- Monitor for activities relating to vulnerable victims from an internal customer reference table including changes that could be indicative of:
  - Change in Power of Attorneys (POA)
  - Financial abuse of elderly people
  - Affiliation with child exploitation
- Identify activities from a new device, location or purchases with an unusual ship to address.
- Use advanced link analysis to show connections to other entities and incidents.
- Suspend suspicious withdraws or transfers until the transaction can be verified.

Key Benefit

Reduce compliance and operating cost

- Process massive volumes of transaction re-validation in configurable batch sizes.
- Straight forward to setup with proven detection models and analytics.
- Flexibility to adapt to evolving Anti-Money Laundering (AML) scenarios and regulations required for all countries without needing to incur any additional development cost.
- Customise scenarios and workflows easily to accommodate unique regulatory requirements in different countries.
- Adapt to anti-money laundering and counter terrorist financing laws and best practices as they evolve.

Use Case

Compliance breaches make headlines which damage brand reputation & result in financial loss

Challenges

- Failure to comply with Anti-Money Laundering requirements can have a significant financial and brand impact on businesses.
- Organisations must find the right balance to meet regulatory obligations without impeding customer expectations and needs.
- The digital economy operates globally but regulatory requirements are often unique in different countries and regions.
- Businesses often have incomplete and inadequate compliance and governance processes.

How Predator 5 Can Help

- Effortless to configure profiles, scenarios and workflows to accommodate unique regulatory requirements of each country.
- Individuals, corporates and other associated entities with suspicious activity can be investigated through dynamic link analysis to establish a clear picture of crime rings.
- Simple process to add items to suspect lists and intelligence files to speed up compliance review.
- Customer view alert triage pane to assist Investigators with due diligence on alerts.
- Configurable dashboard view of alerts to prioritise workload ensuring highest risk is dealt with in timely manner.

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 Predator 5

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, UK, US

GBG | Predator

www.gbgplc.com/apac