



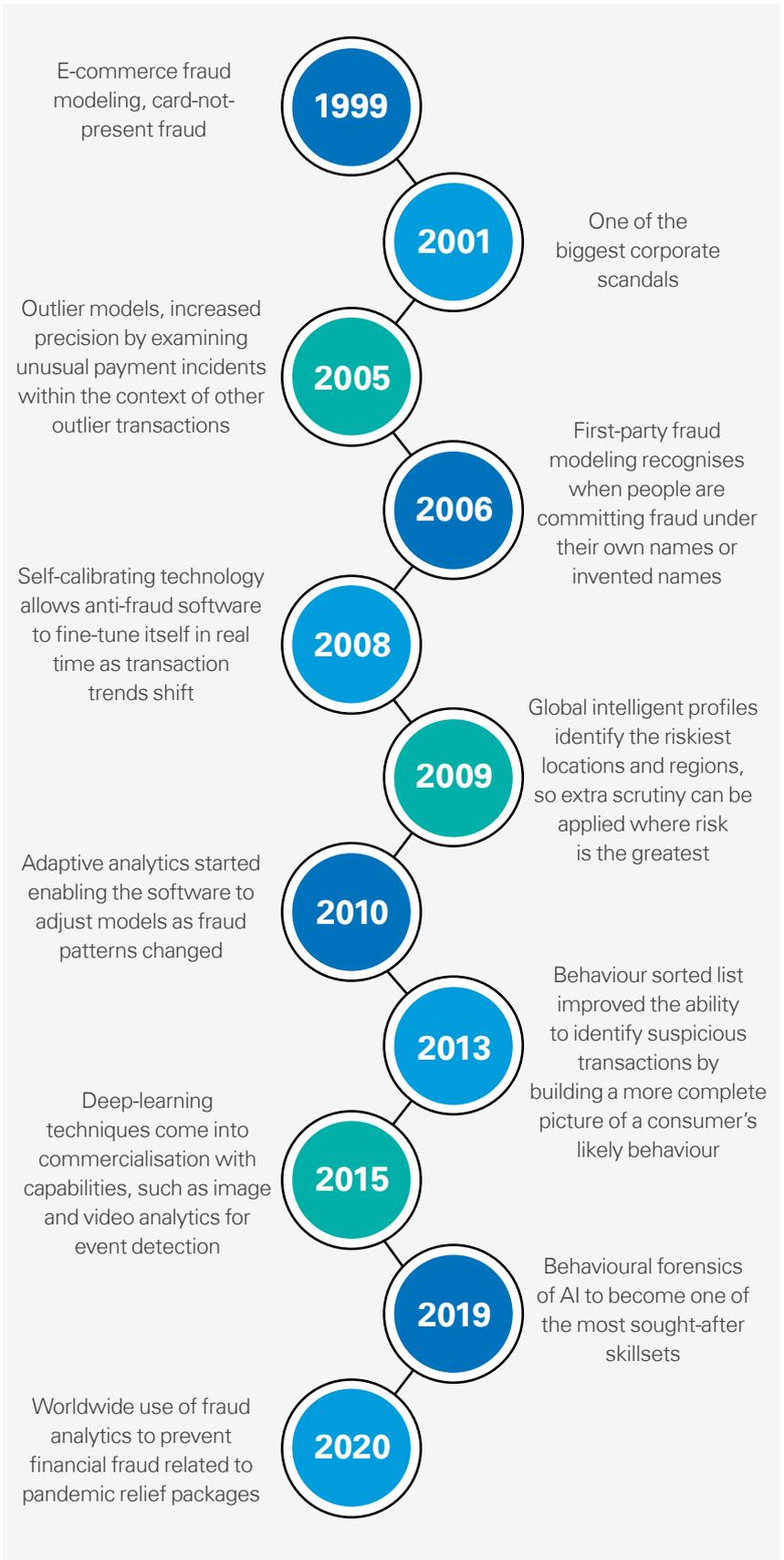
Fraud analytics to combat fraud and improve compliance

home.kpmg/in



Organisations across industries have witnessed a rapid increase in adoption of technology which thereby has generated more data from in their day-to-day operations. This leads to an importance of extracting all possible value from available data sources. Forensic data analytics or fraud analytics is a combination of investigative techniques and analytics which can help organisations to address serious concerns of fraud and compliance issues.

Evolution of fraud analytics



Source: Evolution of Fraud Analytics - an inside story, By T.J. Horan (FICO), KD Nuggets, March 2014



Need for fraud analytics



Push for data driven decisions

Transforming risk and compliance divisions to make data-driven decisions is important to monitor and improve a compliance of any organisation. Fraud analytics can enable such organisations to monitor behaviour and reduce their exposure to high-risk transactions. Fraud analytics assists organisations to identify inherent issues and potential fraud risks in a timely manner, which if not addressed at an early stage, may escalate into a much larger issue impacting their growth and market reputation.

Technological fraud risks

Critical business infrastructure must be kept operational 24/7, which is the key requirement in today's competitive age. The ease of using tools has helped businesses achieve their business goals. It has, however, also opened avenues for fraudsters to exploit potential vulnerabilities.

Rise of structured and unstructured data

The amount of information collected has never been greater, but it's also more complex. This makes it difficult for organizations to manage and analyze their data. A large quantum of data is produced by disparate systems in multiple formats and, hence, it is virtually impossible to get any valuable information from raw data. Data analytics helps in triangulating potentially important information existing in these multiple systems; helps in cleansing raw information and presenting it in a format that is easily comprehensible.

Sectors and indicative analytics

Financial services

- AML and Fraud transaction monitoring
- KYC analytics
- Trade surveillance
- Stressed assets (NPA) analytics

Consumer markets

- Point-of-sale analytics
- Distributor and reseller analytics
- Geospatial analytics.

Manufacturing

- Procurement analytics
- Inventory and goods received note (GRN) analytics
- Sales analytics.

Insurance

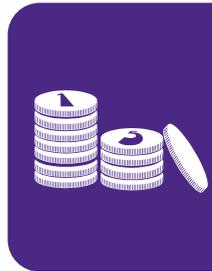
- Agent and policy analytics
- Claims analytics

Life sciences

- Distributor audits/analysis
- Foreign Corrupt Practices Act (FCPA) analytics
- Claims analytics.

E-commerce

- Gross merchandise value analysis
- Logistics fraud
- Returns and refunds
- Promotion codes/vouchers.



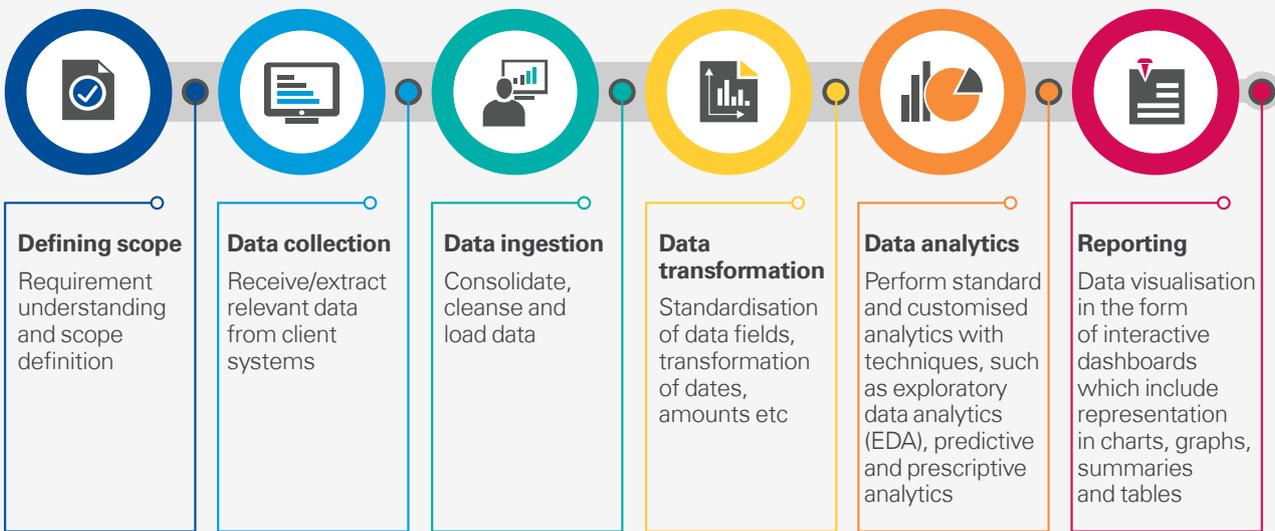
Fraud analytics at KPMG in India

Analytics in fraud detection and prevention



Our fraud analytics professionals are data scientists combined with forensic investigation experience who can tailor technology solutions to your case, for review and analysis of structured and unstructured data on large, complex and high-profile investigations.

We use sophisticated data analytics tools for both analysis and reporting to communicate key findings and help our clients quickly identify patterns and anomalies that require focused review.



Advanced data analytics to detect fraud signals



We leverage on advanced analytical techniques, such as AI, machine learning and natural language processing, along with visualisation techniques, in addition to the traditional ways of executing data analytics using known hypotheses.

Additionally, a geospatial analysis can be performed to locate the existence of a facility/vendor/customer by

extracting geographical data from public sources and correlating it with the information present within the organisation. These techniques, if used appropriately, can go a long way in helping an organisation build a very effective ecosystem that is aligned with the business objectives, can determine anomalies and potential fraud risk.

Fraud analytics in cyber investigations

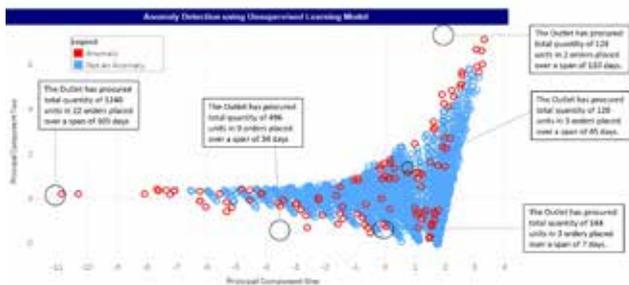


We assist in cyber investigations through analysis of logs (network, VPN, firewall etc.) and datasets across the IT landscape to identify the indicators of compromise as part of cyber incident response.

Advanced data analytics

Advanced machine-learning algorithm to detect fraud

KPMG in India's data analytics team has built and tested the use of an advanced machine-learning model aimed at identifying statistically anomalous sales patterns of outlets. The use of advanced machine-learning techniques helped uncover additional patterns, thereby showcasing how the use of machine learning in fraud detection can immensely impact our approach to fraud investigations.



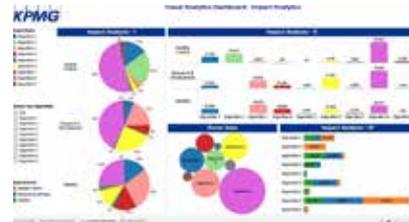
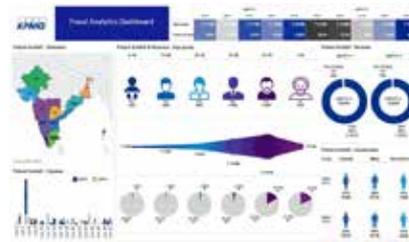
KPMG in India's fraud intelligence platform

Our fraud intelligence platform is a broad-ranging progressive, feature-rich solution, which includes integration with many of the existing ERPs, a data analytics engine and a multi-user review platform. It is an effective solution to detect and automatically alert organisations about suspicious activities or fraudulent behaviour. The solution helps in preventing fraudulent activities before they can move further in a business process, thereby helping organisations avoid significant financial or reputational losses.

Key characteristics

- 1. In-built fraud risk database:** in-built algorithms based on our team's experience from many investigations facilitated across multiple sectors and functions that come as an 'out of the box' solution
- 2. Near real-time fraud risk monitoring:** near real-time monitoring of transactions to ensure timely detection of potential fraud
- 3. Single sign on:** ease of integration with an organisation's active directory
- 4. Flexible and scalable:** can be customised to integrate with varied business processes and scalable to the growing needs of an organisation
- 5. Case management:** in-built automated workflow for multilevel review and detailed investigation of identified anomalous transactions

- 6. Visualisation:** intuitive visualisation and representation of insights identified from the solution
- 7. Advanced data analytics:** ability to leverage on advanced analytical features for effective fraud detection through machine learning
- 8. On-demand investigations and proactive monitoring:** solution for ongoing investigation and proactive monitoring for actionable insights, quicker remediation and decision-making



The images/graphics are indicative and for representative purpose only

KPMG in India's advantage

Our forensic technology lab set-up in Mumbai and Gurgaon in India provide the infrastructure to support wide ranging technological services for clients across the globe.

Our lab facilities include the following:

Fully virtualised



The infrastructure runs on virtualised environment that is scalable and is manageable.

Remotely accessible from anywhere in the world



The facility utilises dual internet connections and can be accessed using strong authentication from any part of the world.

The security is layered with hardening of all components, communication to virtual local area network (VLAN) is allowed on a 'need-to-transit' basis.



Secured with multiple layers of firewalls

The storage is centralised on a SAN with fibre channel connectivity, which can be scaled with minimum disruption of services in production.



More than 50TB of storage available

Research and development



Our labs have dedicated workstations and networks for R&D to provide up-to-date solutions and innovation in the area of fraud analytics, data ETL, computer/mobile/network forensics, live forensics, malware analysis, intellectual property theft, cybercrimes, etc.



Select credentials

Supply chain analytics

Problem statement

The client faced a supply chain fraud wherein goods meant for an organisation at subsidised prices were being diverted and sold in the local market.

How did we assist?

Assisted by analysing the supply chain data, mapping the material movement process of data from tracking batches till the end consumer, thereby identifying and reporting critical process gaps.

Cyberattack – incident response

Problem statement

The client faced a cyberattack, impacting its corporate network by blocking access to data, encrypting files and folders.

How did we assist?

Helped with incident response, fraud analytics, forensic imaging, restoring the cybersecurity schemes, IT asset management and updating standard operating procedures. The team delivered cyberattack investigation results and an events timeline under one consolidated dashboard.

Data analytics of potential siphoning of funds

Problem statement

The client suspected misuse of funds by one of its subsidiaries in India arising due to a sudden change in the business model and procurement patterns.

How did we assist?

Assisted the client by analysing vendor payments, bank books and bank statements, thereby identifying fake vendor payments and fictitious incoming funds.

Review of Anti-Money Laundering(AML)/trade-based money laundering (TBML) system

Problem statement

Management of a multilateral bank decided to conduct an AML/TBML infrastructure review across its global locations.

How did we assist?

Assisted in developing multiple hypotheses and tested them on the transactions performed by the bank. The exceptions were compared with the results of the transaction-monitoring application and reported the identified risks and gaps in the system.

FCPA due diligence

Problem statement

Client requested assistance in conducting FCPA due diligence for their Indian entity

How did we assist?

Using advanced analytics tools and text analytics, the team was able to substantially eliminate transactions which require further review and additional diligence. Advanced visualisation tools were also used for analysis, determining coverage and reporting of results.

Our team

- Our team brings in experience from large and complex engagements involving gathering, analysing and mining huge volumes of structured and unstructured data
- Blended skill sets of accountants, MBA professionals, industry experts, process experts, engineers and technology champions
- A wealth of experience of working with investigators, client staff and their professional advisors across business operations and industry or sector
- Shared methodologies and training amongst professionals in KPMG International's global network of member firms
- Understanding of compliance, law enforcement and regulatory concerns and expectations.



KPMG in India contacts:

Vijay Chawla

Partner and Head

Risk Advisory

T: +91 80 6833 5509

E: vschawla@kpmg.com

Sudesh Anand Shetty

Partner

Forensic Services

T: +91 22 6134 9703

E: sashetty@kpmg.com

Jagvinder S. Brar

Partner and Head

Forensic Services

T: +91 124 336 9469

E: jsbrar@kpmg.com

Muntazar Sayed

Technical Director

Forensic Services

T: +91 98 1965 5859

E: muntazarsayed@kpmg.com

home.kpmg/in

Follow us on:

home.kpmg/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only. (037_BRO0820_SP)