BLACKSWAN
TECHNOLOGIES

# Digitisation in FinCrime: Anti-Fraud and AML

*Why organisations standing still are making it easier for bad actors to evade detection*

This whitepaper underlines the challenges that banks and other financial service providers are facing in regards to fraud and money laundering, with a particular focus on:

- The changing regulatory landscape
- Drivers for new technology
- The advanced techniques that provide a solution for banks
- Next steps for banks

# INTRODUCTION

Financial institutions maintain two large and complex operational programmes dedicated to tackling financial crime compliance - for fraud and money laundering. Both utilise technology operated by specialists that are dedicated to rooting out criminal activity. The two regimes are distinct; fraud is about the manipulation of records to illegally extra funds, while money laundering is about laundering funds to obscure their origin.

Despite the differences in operational requirements for technology, banks face similar pressures and challenges with fraud and money laundering. Many banks are still using manual methods and inflexible control systems - increasing pressure on their staff to keep up with regulatory changes. Regulators have increased scrutiny on firms around their AML and anti-fraud controls with new laws, extensive investigations, and rising fines, and this has provided the impetus for banks to invest in new capabilities that can assist them in complying with regulations. This paper will look at the current trends, drivers for new technologies and the innovative techniques that banks can use going forward, firstly on Fraud, and then AML.

**Table of contents**



# INNOVATIONS IN FRAUD DETECTION

## Trends

Financial fraud has grown exponentially with the acceleration of digital banking due to the COVID-19 pandemic. According to Juniper Research, record numbers of online payments were processed last year and this trend is bound to continue. The report predicted that digital wallet users will exceed 4.4 billion globally in 2025, up from 2.6 billion in 2020. As transaction volumes surge, cybercriminals continue to discover new and complex ways to circumvent existing anti-fraud systems and financial institutions are struggling to keep up.

Last year, fraudulent bank transfers and payments resulted in unrecouped losses of £783.8 million in the UK according to UK Finance; and $314 million in the US according to the Federal Trade Commission. While financial services firms have managed to prevent some amount of attempted unauthorised fraud, existing systems are incapable of handling the increasing sophistication of fraudulent activities. Thus, **firms continue to invest in advanced technologies to improve the detection, prevention and investigation of fraud attacks.**

Current systems fail to depict a holistic view of fraud risks and exposures during investigations due to data silos. And with information overload, these systems are less effective in analysing large volumes of data to identify suspicious behaviours and patterns. The ever-evolving fraud landscape also makes it more difficult to identify new fraudulent schemes, since **existing systems are mainly rule-based and configured to detect only known scenarios**. Rule-based systems also result in high numbers of false positives that require manual investigations.

Regulators are also taking measures to safeguard financial institutions and their customers through advisories and new regulations. Digital identity, data privacy, and data protection have been of particular concern. Most recently, the Digital Identity Act of 2021 was introduced to protect US consumers against identity theft and online fraud through secure methods of digital identity verification; the Financial Action Task Force (FATF) released guidance on Digital Identity with best practices for financial institutions that use third parties to meet identity verification requirements; the National Institute of Standards and Technology (NIST) published its data privacy framework to provide the financial sector in the US with best practices; and the Data Protection Act of 2021 was introduced to ensure that firms take adequate measures to protect their customers' data privacy.

## Drivers – increasing volumes, costs & attack sophistication

Banks are under pressure to combat fraud in order to prevent significant financial losses in addition to reputational damage and resource wastage, they are facing several particular challenges:

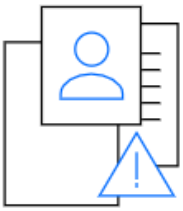
Fraud attacks are growing more sophisticated as bad actors use increasingly complex tools and methods to coordinate attacks, such as combining bot-powered and manual methods, blending fraudulent and legitimate transactions, and utilising cloud services for greater scale.

Transaction volumes are increasing substantially, requiring analysis of massive amounts of data during fraud investigations. However, current systems are mainly rule-based and inadequate in orchestrating data from multiple sources to supplement investigations.

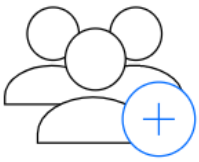
Compliance costs are rising as firms scale their task force to handle surges in demand for financial services by hiring more personnel and training staff. This is in addition to accounting for increasingly stringent regulatory requirements across multiple jurisdictions.

## Techniques – behavioural, network and login analysis

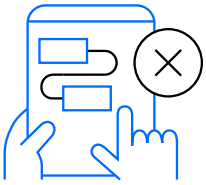
While the majority of current anti-fraud systems are rule-based, there are several other methods that can be used to further enhance detection and investigative capabilities. These include:



**Behavioural analysis** generates patterns and predicts the acceptable activity for each customer by using data mining and natural language processing to analyse existing profile data including KYC information and transaction history. Customer profiles can be further enriched with structured and unstructured information from global news outlets, social media, company profiles, the dark web, and other sources.



**Network analysis** identifies relationships between all entities involved in transactions, including hidden connections between organizations through mutual managers, common shareholders, common counterparties, and unrelated counterparties by tracking the flow of funds and analysing KYC information, transaction history, global news outlets, social media, company profiles, and the dark web. A data mesh architecture, featuring heterogeneous data formats and distributed data sources is well-suited to underpin the network analysis.



**Login analysis** detects suspicious logins by IP network providers outside the country of the customer by examining the transaction login history for unusual times and durations, such as after midnight and with a duration less than 3 minutes. This may include logins by several IP addresses and from different locations, as well as the common IP address logins of different customers.

## Scenarios

### Scenario #1: Bank account takeover identified through network analysis

A fraudster gains access to a person's pre-existing account with ACH information and other credentials obtained from a stolen check. The fraudster transfers the funds from the victim's account to an intermediary account then cashes out through ATM withdrawals. With network analysis, the bank can identify the lack of association with the intermediary account based on the victim's transaction history. And with login analysis, the bank can identify the unusual login based on the fraudster's IP address.

### Scenario #2: Credit card fraud detected using behavioural analysis

A fraudster gains access to a person's sensitive information that has been exposed through a data breach of an online retailer. With the victim's name, account number, and card security code, the fraudster makes multiple back-to-back online purchases. Using behavioural analysis, the bank can detect the fraudster's unusual shopping patterns based on the types of purchases, unusual amounts, and sudden surge in frequency. The bank can then notify the victim in near real-time with phone-based alerts.

# INNOVATIONS IN AML

## Trends

While AML is the second pillar of financial crime prevention, it has its own idiosyncrasies to address. There is room for improvement in tackling money laundering; the United Nations (UN) estimates the amount of money laundered globally to be 2-5% of all global GDP yearly, or $800 billion - $2 trillion, a staggering sum that goes to show criminals are evading detection by banks and other money service businesses (MSBs) such as check cashiers and international remittances, far too frequently.

The National Crime Agency (NCA) suggests that money laundering costs the UK economy around £24 billion every year and in 2015 the NCA estimated that at least £1.5 billion in criminal proceeds are laundered through banks and other money service businesses (MSBs) in the UK yearly. Due to increasingly stringent regulations, money launderers have looked elsewhere to funnel their illegally made profits and many have turned to MSBs as conduits through which they can deposit cash. More recently, the UK regulator, the Financial Conduct Authority (FCA) threatened to take action against retail banks over persistent AML failings. It highlighted several key control weaknesses in the following areas: governance and oversight, risk assessments, due diligence, transaction monitoring and suspicious activity reporting (SARs). Regulators have also been providing guidance and updating requirements related to Ultimate Beneficial Owners (UBOs).

**The traditional monitoring capabilities of banks are largely retrospective**, using rules and transaction-based methods in an attempt to detect suspicious activity and prevent money laundering. The information is then compiled into regulatory reports such as SARs and sent to financial investigation agencies to support wider government efforts to combat money laundering.

**The risk-averse nature of banks leads to them filing far too many SARs,** costing both them and law enforcement agencies. The retrospective type of traditional AML software in use at many banks has resulted in an inefficient system for alerting human investigators. For example, due to the complexity, lack of automation and time associated with enquiring into the origins of such alerts, false positives are far more prevalent than would ideally be the case. The rule sets to detect known scenarios are often not configurable, and banks have lacked the relevant data from investigating bodies, along with the ability to use their own existing internal data to power feedback analytics, which would greatly assist in their ambition to uncover and stop money launderers.

## Drivers – difficulties in detecting complex criminal networks

Regulators increase requirements for banks to effectively detect suspicious behaviour and scrutinise clients - or face hefty fines and a dent to their reputation. However, they have to deal with a number of key challenges:

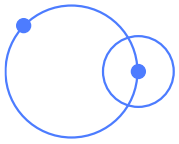
Criminals have been using increasingly sophisticated methods to evade detection - operating across complex networks, using virtual currencies as a vehicle for money laundering and therefore benefitting from the anonymity it provides.

Many AML compliance decisions continue to be made manually by firms. This is a time-consuming, resource-intensive method of investigation which is costly and results in a high rate of false positives, making the process ineffective and inefficient. Using human analysts for all decision-making can also detract from higher risk events.

Criminal organisations operate between multiple networks, all of which are complex. Firms have to use internal and external data sources effectively but are held back from transactional data being held in legacy systems and a lack of government data to hand. In addition, they're tasked with monitoring large and complex data sets without automated monitoring, alerting and reporting capabilities.

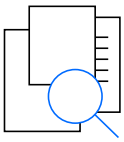
## Techniques – link analysis, behaviour and relationship monitoring

While current AML methods include retrospective, rules-based and manual processes, there are numerous advanced techniques banks should adopt to stop money launderers. These include:



**Visual Link Analysis** enables banks to visualise and discover relationships and hidden patterns heaped in millions of transactions, relationships and events, consolidating data fragments residing in multiple silos. Find hidden relationships among a combined set of structured and unstructured data, and enrich, manage, visualise and investigate entities of various types such as holding structure, functionaries and addresses.

As well as the creation of advanced rule-based scenarios, new techniques involve **behaviour and relationship-based monitoring.** Relationship-based monitoring discovers complex networks of shell companies that support money laundering on a global scale, which are often difficult for conventional systems to detect. Plus, behaviour-based monitoring counters launderers' efforts to remain undetected by rule-based scenarios in standard AML solutions. Together, these new monitoring techniques enable the retirement of many unproductive workflow scenarios, resulting in increased precision of alerts and a significant decrease in the ratio of false positives.



**Front/Shell Company Identification** using multiple sources, including open, paid and internal bank sources to create an enriched entity knowledge graph for every suspected company. Knowledge graph attributes are factored by an editable, best practice, scoring and disqualification mechanism, and includes company locations, holding structures, online indicators and financial indicators. All indicators and diagnostics are scored by a final scoring algorithm. An enhanced, single consolidated view of entities can be provided through a data mesh architecture.

## Scenario

**Use of Shell Companies to mask activity**

An arms dealer inflates the invoice value of used cars and ships them between shell companies, creating a complex network masking the identity of the criminal organisation, and enabling it to easily launder money through various bank accounts. A bank can detect simple and complex networks of shell companies by using a data mesh architecture to pull transaction and customer data held across the organisation, as well as data from open source intelligence and paid sources. The data can be then used to analyse transactional activities, UBOs, addresses, etc. via knowledge graph link analysis. Visual link analysis can then be used to uncover further links with other criminal parties. Detection of suspicious activities using pre-defined explainable and creatable features that are based on money laundering and terrorist financing behaviours, greatly reduce the false positive alert ratio and decrease the overall risk.

# BLACKSWAN'S APPROACH

While some financial institutions have managed to integrate their AML, fraud, and security operations, technological convergence has remained a challenge. Yet, adopting compliance innovation too conservatively has its own issues, not least the increasing sophistication of bad actors identifying gaps in risk monitoring.

BlackSwan addresses this issue with its Financial Crime Compliance (FinCrime) product, ELEMENT of Compliance™, by offering the full range of intelligence and workflows to support financial crime compliance, including KYC, Perpetual KYC/EDR, Watchlist Screening, Adverse Media Monitoring, Transaction Monitoring, and Transactional Intelligence.

BlackSwan Technologies' ELEMENT of Compliance™ is a leading application in the FinCrime sector recognised by Chartis Research, an industry analyst firm dedicated to risk and compliance. Chartis took special note of the innovativeness of the platform's artificial intelligence technology, particularly its revolutionary Knowledge Graph to powerfully represent entities, relationships and transaction behaviours.

ELEMENT of Compliance challenges traditional approaches to Fraud/AML by combining all available sources of information with AI/Cognitive Computing capabilities to automatically infer insights, strengthen team decision-making abilities and enhance operational efficiencies. With built-in machine learning, the application automatically adapts with experience and new patterns. Highlights include:

- **End to End AML / Anti-Fraud / KYC / Customer Lifecycle Management Solution:** Incorporates data acquisition, rules engine, pattern diagnostics, alert generation optimisation, alert management, workflow, and case management.
- **Single, consolidated view of entity via a Data Mesh:** Achieve a single view of any entity through a Data Mesh architecture which integrates data across the entire enterprise, democratising access to the data regardless of location, whether it's at rest or in motion. Knowledge graph technology enables the enrichment and visualisation of entities, transactions, direct relationships, non-obvious relationships, and networks.
- **Continual insight improvement:** By applying structured and unstructured machine learning, generate powerful insights that enable analysts to quickly identify risks and repeated patterns – allowing faster and more informed decision making. The application can monitor the outcomes of alerts and investigative cases handled staff and automatically, continuously improve the quality of its assessments and recommendations.
- **AI Automation** including alert triaging, alert grouping and insight creation, enables the creation of advanced versions of rule-based scenarios as well as complex network & relationship-based scenarios.

# INDUSTRY RECOGNITION


The Risk Technology Awards 2021 have named BlackSwan's application, ELEMENT™ of Compliance, as the Anti-Money Laundering Product of the Year *and* Anti-Fraud Product of the Year.


BlackSwan Technologies has been recognized by Chartis Research, the top research provider for the risk technology market, as a Leader in Know Your Customer (KYC) and anti-money laundering (AML) Solutions in the "KYC/AML Software Solutions, 2020: Market Update and Vendor Landscape".


In its annual report of "must watch" emerging technologies, Gartner has named BlackSwan Technologies as an enterprise artificial intelligence leader that is redefining the industry. BlackSwan Technologies is a pioneer in what Gartner refers to as "Composite AI" — the combined application of different AI techniques to improve accuracy and efficiency and "bring AI closer to human learning and intelligence."

# ABOUT BLACKSWAN TECHNOLOGIES

**BlackSwan Technologies** is a PaaS/SaaS product company. Its enterprise software **ELEMENT™** serves as a business operating system powering the rapid development of enterprise AI applications that mimic the cognitive functions of human intelligence. ELEMENT, and applications built with it, can be used by enterprises to collect and organise massive amounts of data, detect risks, enhance decision-making, and more. Pre-configured applications have been tailored for specific sectors and business functions, including financial crime compliance, underwriting risk management, and cyber-security risk monitoring. BlackSwan's offerings are trusted by some of the largest global organisations.

ELEMENT's key differentiators and value proposition include:

1. **Any Data Source**
   ELEMENT can connect to any structured or unstructured, internal or external data source, regardless of volume, velocity, variety and/or veracity of data
2. **Schemaless Knowledge Graph**
   Dynamically and self-sufficiently fit to any model, entity, relationship, attribute or context to manifest any business application, while emphasising the customer unique value proposition
3. **Low/No Code Whitebox**
   Fully open for configuration, expansion and integration, optimising utilisation of existing assets, ensuring self-sufficiency, and future readiness, with little to no expertise required
4. **Composite AI**
   Accommodate any algorithm and generate any insight to address any business challenge, using Out of Box, bring-your-own, or train custom AI models using state of the art transfer learning, Deep Learning, NLP, Graph Computation and Machine Learning. Democratise AI and deploy it at scale.
5. **Cloud Agnostic PaaS**
   Cloud native PaaS Enterprise Operating System Platform, providing military-grade security, regulated privacy, and mission-critical resilience, with seamless scaling to budget for licence and infrastructure costs
6. **Data Mesh Architecture**
   Data assets do not need to be pulled or replicated into a single uniform repository. Instead, a Data Mesh makes them discoverable and accessible where they originally reside. This architecture design is better aligned to the decentralised nature of data found in organisations today. This helps enterprises to build knowledge graph applications quickly, removing a key barrier to using AI applications and reducing complexity.

BLACKSWAN

TECHNOLOGIES