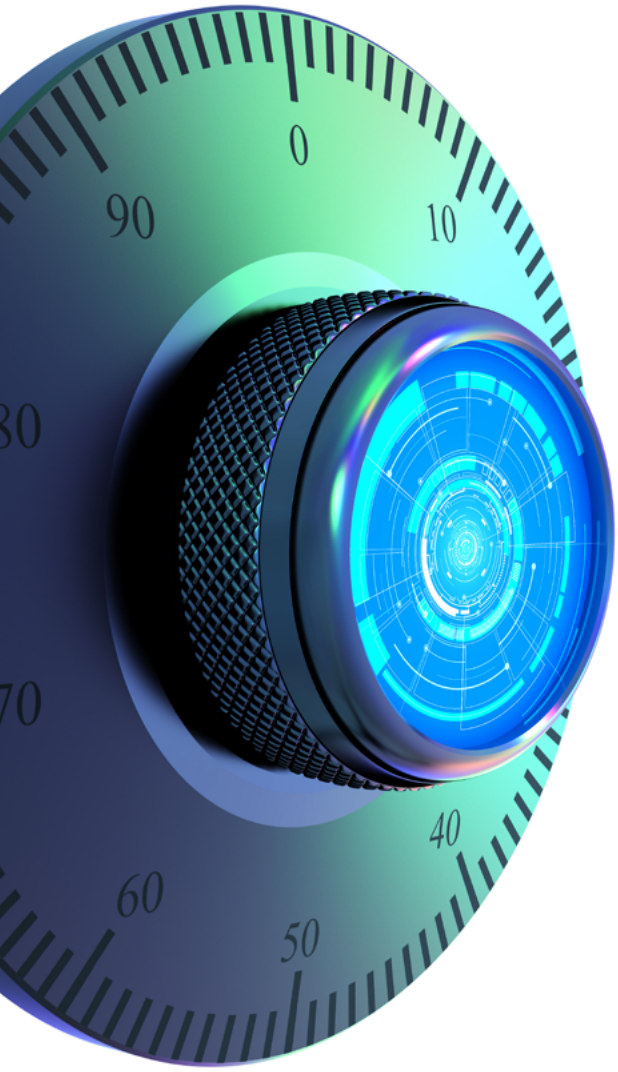
accenture



FINANCIAL CRIME

DATA SCIENCE TO THE RESCUE

FS PERSPECTIVES

CONTENT

With the changing nature of crime and a rapidly evolving regulatory landscape, financial institutions globally are turning to data science to fight crime and manage compliance.

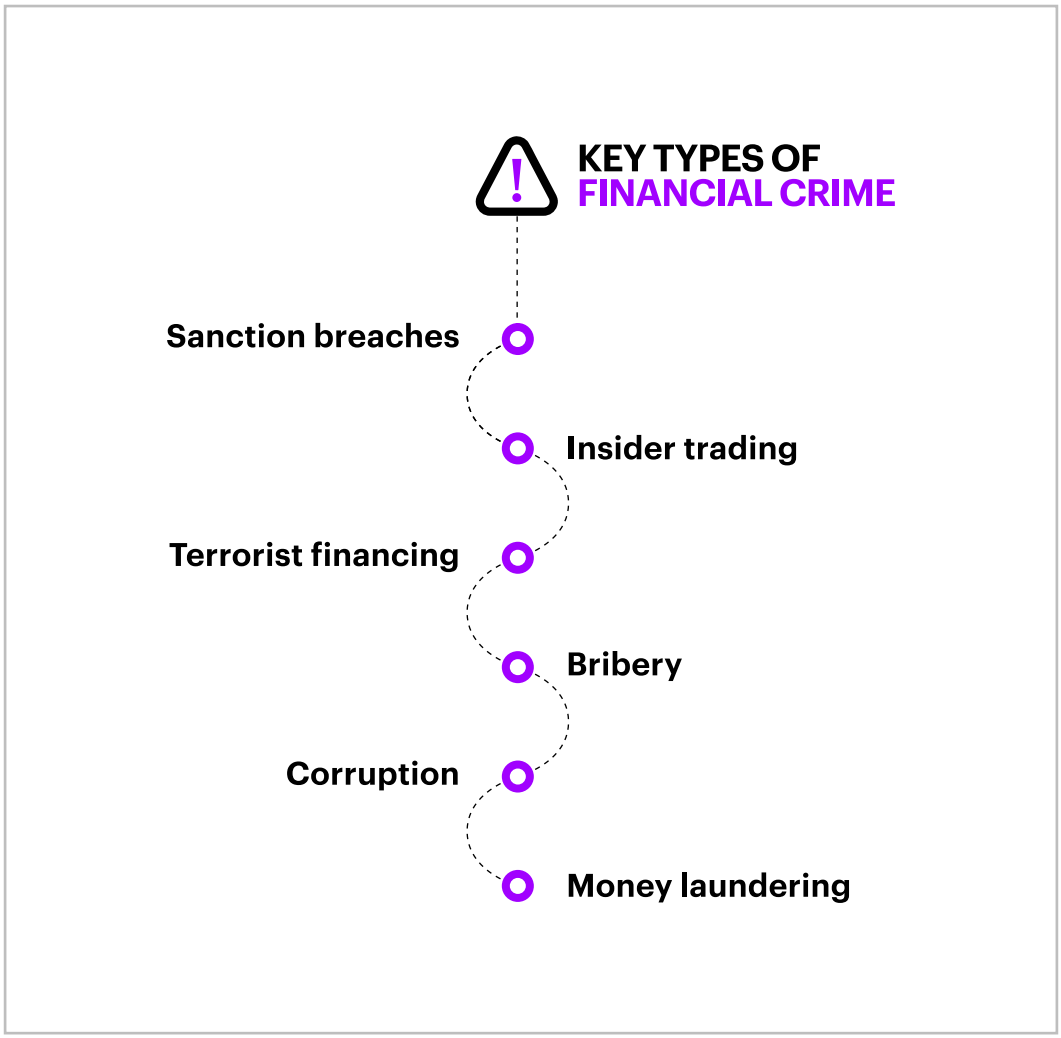
The financial crisis of 2008 changed the world. Its impact was not limited to the financial sector, rather it had a ripple effect on industries and businesses globally. The crisis revealed weak policies that led to deep cracks that threatened to collapse the global financial system. While there was a lot of learning for the sector, banks faced a new challenge—ensuring compliance with new regulatory requirements to prevent future crises. Over this past decade, financial compliance has evolved in many ways, changing how we work and pushing the boundaries of innovation to develop the technology and strategies required to thrive in this new regulatory environment.

Amid growing regulatory pressure, advancements in technology and new capabilities to interpret large volumes of data, data science is emerging as the strongest ally for firms looking to transform their Financial Crime Compliance operations.

FINANCIAL CRIME COMPLIANCE

Over the past few decades, financial crime has been rising, not just in number but also in sophistication. It has become a growing concern for governments and financial institutions the world over because it can lead to enormous monetary losses and damage an organisation's reputation. The loss of revenue through criminal acts, such as corruption, tax evasion and money laundering, can hamper societies' economic development and even threaten their stability.

2–5% of the world's GDP ($800 BN–$2 TN) is laundered each year.[1]



[1] United Nations Office on Drugs & Crime

A STEP IN TIME SAVES DIMES

For financial institutions, this translates to taking proactive steps to safeguard themselves. Today's Financial Crime Risk Management is characterised by a reactive, rules-driven detection approach fuelled by response to regulation. With the evolution of the financial landscape and advancement in technology, financial institutions must adopt a proactive approach, driven by technology, to detect and deter financial crime.

However, several challenges prevent institutions from securing themselves.

LEGACY SYSTEMS

Most financial institutions are struggling with legacy systems even as fraudsters take advantage of new technology to hide their crimes. Banks need to upgrade their technology if they want to take financial criminals head-on.

NEW CRIMINAL TOPOLOGIES

Crime topologies are changing as are the channels through which crime is being committed, e.g. automated teller machine (ATM), mobile platforms and crypto-currency. These trends need to be understood and channels secured to mitigate potential risk to business.

COMPLEX COMPLIANCE LANDSCAPE

Financial institutions are spending an average of $60 million per year (larger firms spend up to $500 million) on meeting Financial Crime Compliance requirements.

EVOLVING FINANCIAL LANDSCAPE

The combination of new threats, high transaction volumes and increased regulation places a premium on a financial institution's ability to streamline operations and maintain appropriate levels of control.

CRIMINAL INNOVATION

New criminal techniques across the financial crime spectrum are continually emerging and becoming ever more sophisticated.

To address these challenges, banks need to embark on a journey towards building proactive, data science-driven capabilities. They must embrace an integrated approach to threat identification, using innovative technology and component-based architecture to combat financial crime.

WHAT'S DATA SCIENCE GOT TO DO WITH IT?

Data science has evolved from statistics to include concepts and practices such as artificial intelligence (AI), machine learning (ML) and deep learning. While institutions are collecting and storing more data as its availability increases, they also need to find new ways to analyse this data for risks.

THE EVOLUTION OF DATA SCIENCE

Much of the growth in data analytics is from the fintech boom, led by top digital payments firms. These firms leverage analytics to not only digitise cash payments but also scale their customer base and interpret customer behaviour.

On the other hand, financial institutions are also fast realising the potential of data and how they can leverage it to improve consumer experience, create efficiencies, explore new markets and manage risk. Using techniques such as AI, ML and blockchain, banks can analyse data and use the insights to simplify decision-making across their operations. Harnessing the power of real-time data analysis can help financial institutions address fraud more effectively to better monitor transactions and make decisions quickly.

In line with the growth of data (within the bank, with regulators or from third parties), the scope for data science has grown tremendously.

TECHNOLOGY INNOVATION, THE RIGHT WAY

Criminals are constantly innovating and experimenting with new techniques to commit financial crime. In response, firms too must develop ever-more sophisticated techniques to uncover and stop new threats. Technologies that are transforming the approach to the prevention, detection and management of financial crime are as follows:

BIG DATA

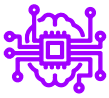
Transform compliance functions, including enhanced data collection and advanced risk detection, using big data-led predictive analytics

BIOMETRICS

Measure and analyse unique physical or behavioural characteristics to transform customer experience during onboarding or for authentication at the point of payment

NATURAL LANGUAGE PROCESSING (NLP)

Enable advanced financial crime detection and management by introducing natural language processing (NLP) and text analytics alongside ML models and RPA



MACHINE LEARNING

Reduce false positives and drive the detection of new, sophisticated typologies and techniques

ROBOTIC PROCESS AUTOMATION (RPA)

Automate repeatable, large volume activity and / or data collection and presentation to investigators

BLOCKCHAIN

Prevent and detect financial crime due to an irrefutable and unchangeable record of past transactions

NETWORK ANALYSIS

Analyse massive transactional data to reveal hidden patterns and relationships

CLOUD

Use technology solutions that will support, grow and evolve as the complexity and importance of analytics approaches and modelling increase

ENCRYPTION

Enable data sharing without exposing the underlying data, using homomorphic encryption, thus providing the compliance required by regulators and privacy by customers

HOW DATA SCIENCE CAN HELP

The adoption of data science in financial crime compliance has grown significantly over the last decade, from being a “trend to watch” at the start of the decade, to experiments with the technology and pilots in more recent years. It has now been deployed in live operation in a number of banks. While still at early stages in moving toward full potential, its benefits are being seen in actual use cases.

Most banks today are seriously evaluating plans to adopt data science. Globally, about one-fifth of banks have already invested in leveraging the technology in a production environment.[2] Another 50% of banks are actively interested, split evenly between institutions in the more advanced trial stage and those that are actively planning. The overall consideration is high, with only 10–15% of banks across regions, and across financial crime and compliance, not interested in advanced analytics. This clearly indicates that there is an enormous potential for analytics in the banking sector.

[2] Oracle - Assessing the Role of Big Data in Tackling Financial Crime

Here's a look at some use cases of data science in the financial crime and compliance management space:

USING NEW DATA SOURCES

Banks are using new data sources to improve fraud detection and cybersecurity, particularly for online banking. For instance, web session data can be used to profile users and find usage patterns. This approach uses machine-generated log data and message transmission from web sessions, (i.e. clickstream data) to understand the paths a user takes when visiting websites. It can be used along with other anti-fraud approaches to identify actions that may indicate fraudulent access, e.g. whether the payee for the new payment instruction is in line with previous patterns. The bank can then impose additional security validation checks.

CREATING A DATA LAKE TO RESPOND TO REGULATORY DEMANDS

US banking institutions have created a central data-as-a-service platform using a data lake approach, for managing regulatory information requests, particularly those relating to regulatory Matters Requiring Attention (MRA). Such platforms usually store all relevant data using Hadoop (along with relational databases). They also usually have an analytical workflow orchestration layer that manages data quality, processing, model execution and reporting.

WORKING WITH FULL DATASETS TO ANALYSE POTENTIAL FRAUD

Data science also helps banks enhance credit card fraud detection. Most banks run real-time basic checks on transactions based on predefined rules and then run batch analysis using more sophisticated models overnight. This lengthy process focuses on only high-value transactions and/or uses a sampling of data over time to detect trends. From a statistical modelling viewpoint, fraud is a rare event detection issue, which means that missing positive fraud cases can have a significant negative impact on model quality. Major banks are now using Hadoop to analyse daily transaction volumes, instead of just above-the-line transactions. This not only enhances detection efficiency but also reduces computing costs and analysis run-time.

DISRUPTING THE FRAUDSTER'S LEARNING CURVE

To protect their businesses from financial crime and prevent fraud, firms need to advance security capabilities, be better informed and stay one step ahead of sophisticated cybercriminals. This means banks need to detect and adjust behavioural models to events with a low degree of latency. Using tools such as Apache Spark can help banks by processing streaming data transactions in a real-time setting. Spark also allows models in the background to be continuously updated.

TRANSFORMING COMPLIANCE WITH DATA SCIENCE

SUPERVISED AND UNSUPERVISED ML ALGORITHMS ALONG WITH DATA SCIENCE CAN IMPROVE REAL-TIME FRAUD SCORING

- Datasets are created by extracting information from online sources and enterprise systems, including documents in natural language.
- ML models search these large datasets to spot and detect fraudulent transactions. Solutions monitor transactions in real time to identify gaps, issues and trends in financial crime.

WORD COMBINATION	FRAUD PREDICTION
suspicious, vague, black market	Positive
reliable, love, great store	Negative

- NLP algorithms search for these word patterns /combinations to predict suspicious behaviour.

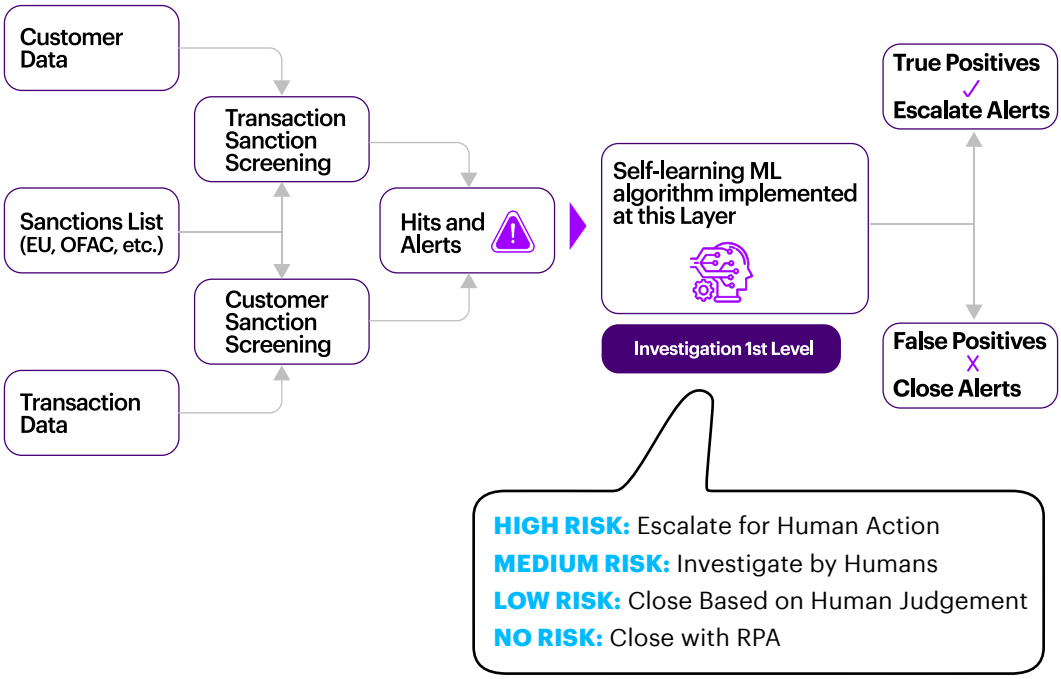
OUTCOMES / BENEFITS

Reduce false positives in fraud detection

Keep up with ever-changing, sophisticated fraud techniques

Identify patterns / connections invisible to the human eye

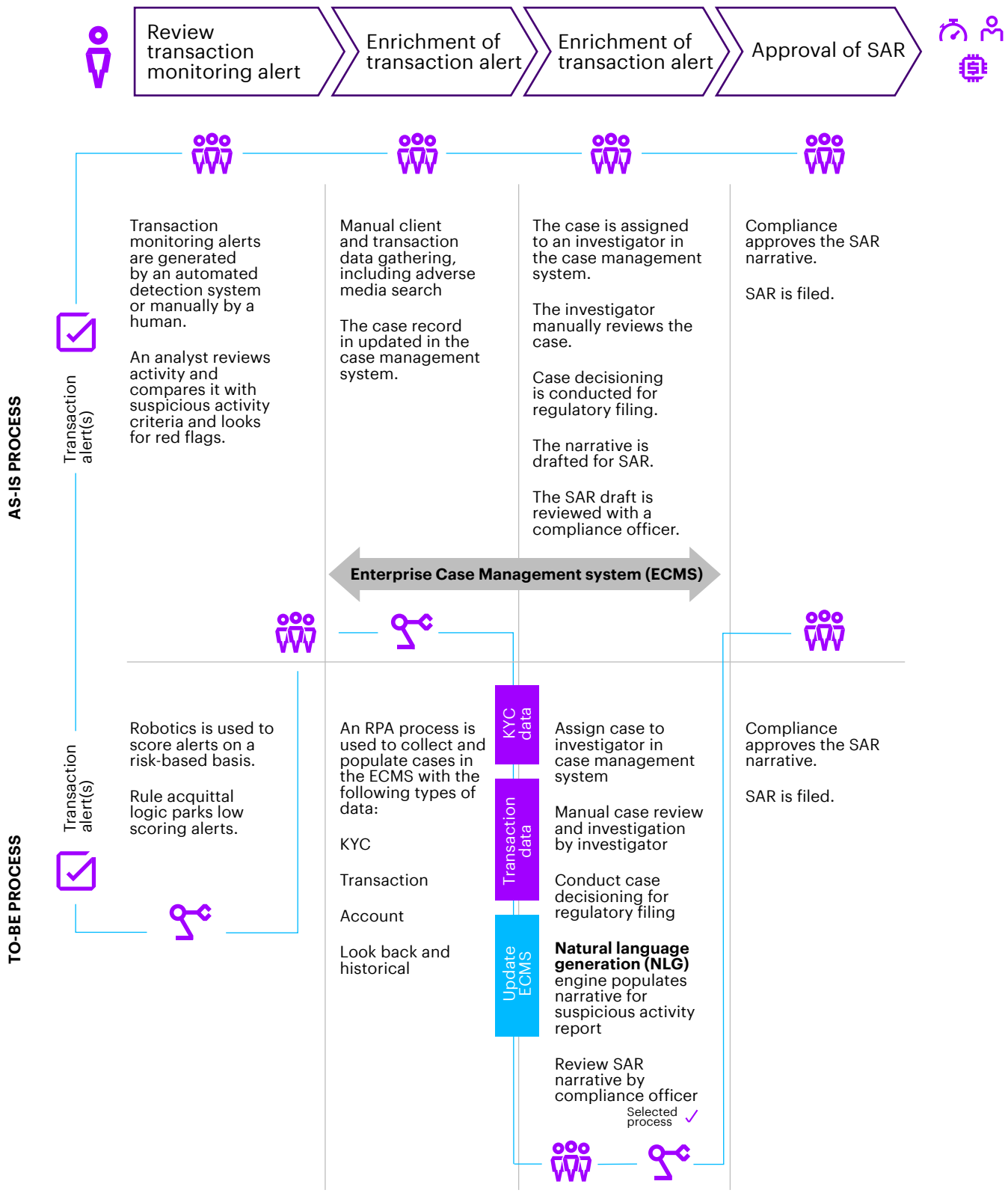
AI AND DATA SCIENCE PROVIDE THE FIRST LEVEL OF INTELLIGENT ALERT MANAGEMENT TO IDENTIFY FALSE POSITIVES



AI and RULES-BASED MODELLING

- AI analyses alerts by name and location matching strength, rarity of the name in customer population, historical match rate, and true match and false positive rate analysis.
- RPA sources additional data for analysis, working together with the AI engine.
- Clear false positives are closed using rules-based classification.
- AI categorises alerts and RPA routes cases to human operators.

Using NLP, AI, data science and automation for an anti-money laundering (AML) compliance program for suspicious activity report (SAR) generation



Average cycle time reduced by 40–50%

THE DATA (SCIENCE) DEAL FOR COMPLIANCE

Leading financial organisations must adopt an intelligent approach towards financial crime that has data and analytics at its core. New technologies and solutions are making it easier for banks to not only create integrated datasets, but also analyse this data to generate useful insights that can help prevent and detect financial crime. The following elements are needed to manage evolving risks to assets:

DATA VISUALISATION

Data visualisation techniques allow decision makers to view complex data through a visual interface, making it easier to identify visual patterns and inconsistencies.

PREDICTIVE MODELLING

Predictive analytics involves interpreting data to make informed predictions about future events. It provides businesses with near real-time and more accurate forecast reporting so that they can make more informed business decisions. It is the most powerful technique for detecting financial crime, especially for large populations of clients or transactions.

SOCIAL NETWORK ANALYSIS

Financial crime cases are often not isolated incidents but rather part of a network of actors. Social network analysis helps to investigate if a financial crime case is part of a much larger network. Both social network visualisations (relations between actors) and social network statistics (nature of these relations) are valuable in disentangling financial crime networks.

ANALYTICS-BASED ENTITY RESOLUTION

Analytics-based entity resolution can generate a single view of a customer maintaining multiple identities and relationships across a bank. The bank does not need to overhaul any of its disparate legacy systems that hold customer data. Sophisticated analytics are used for such matching and sometimes augment bank's data with that of external third-party data to arrive at accurate matches. The entity analytics solution links the data available in the bank, such as unstructured customer data in the form of mails and chats, with that available in external sources, including social media and web-based information, to mine suspicious criminal networks. Banks can then flag such networks for further scrutiny.

QUALITY DATA

The quality of insights depends greatly on the quality of data used. Financial services firms use a variety of internal and external data sources, but many firms – particularly universal banks operating in different regions and across different lines of business, using multiple systems and data sources – face data quality issues.

To improve data quality, banks must:

- Define the right data quality metrics
- Establish central data screening and reconciliation
- Improve data governance

RIGHT DATA

For most organisations, lack of data is not the problem. The real problem is lack of the right data. Banks typically have access to centralised data, but most use less than 5% of the available data for making decisions related to financial crime prevention. The rest of the data is mostly considered too expensive to deal with.

Banks must follow a three-step process to get the right data:

- Understand the data they need to prevent fraud
- Use technology to obtain the right data
- Analyse the information to generate insights

KEY FACTORS TO CONSIDER

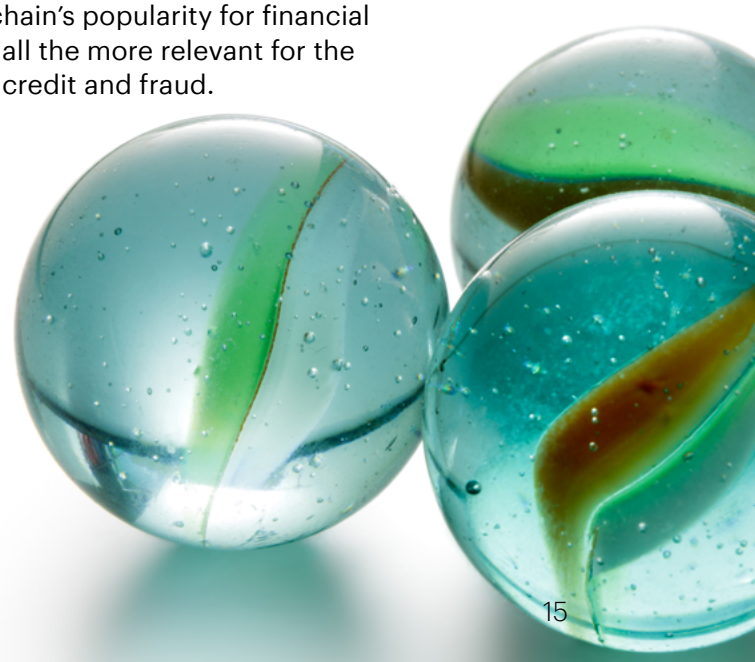
IMPACT OF GENERAL DATA PROTECTION REGULATION (GDPR) ON FINANCIAL CRIME COMPLIANCE AND DATA ANALYTICS

Financial services firms often act as "controllers" of the personal data they collect on customers and counterparties. Controllers are obliged to respect and facilitate the privacy rights of individuals, or "data subjects," under the GDPR. As financial crime compliance efforts involve the analysis of personal data, the data restrictions may represent a challenge for financial institutions. GDPR compliance penalties can reach up to €20 million (or 4% of global revenue).

BLOCKCHAIN MAY HOLD THE ANSWER

Blockchain, the technology that underpins Bitcoin, has caught the attention of bankers across the globe. Blockchain as a whole is a double-edged sword for the financial industry – Bitcoin's potential for money laundering is well-known. However, certain blockchain variants are likely to be championed by banks. Banks have been looking at payments-related use cases for some years, and this will only continue to grow (especially with increased use of features like smart contracts and proof of authority).

On the data science side, blockchain will also have a role to play. What data science has done for predictions, blockchain may do for data integrity. Blockchains are designed to be authoritative sources of information (with their focus on capturing timestamps and being tamper-proof), and adoption of blockchain for more purposes would make more reliable information available for analysis and predictive modelling. Blockchain's popularity for financial transactions and proof of ownership make it all the more relevant for the banking industry, as such data are useful for credit and fraud.



DATA SCIENCE, FINANCIAL CRIME COMPLIANCE & ACCENTURE

Accenture's Compliance Framework comprises capabilities and features especially designed to drive value, reduce costs and future-proof our clients' businesses.

accenturestrategy
accentureconsulting

FINANCIAL CRIME TRANSFORMATION

Transforms Financial Crime functions by designing and implementing new Financial Crime operating models, processes and Data Science technologies to substantially reduce cost and increase compliance.

- Strategic Cost Reduction
- Operational streamlining
- Technology solutions
- Staff restructuring

accenturetechnology
accenturedigital

FINANCIAL CRIME ANALYTICS

Applies advanced data analytics to detect and investigate suspicious and unusual behaviour, and understand and respond to customer risk. Intelligent Financial Crime Detection solutions leverage Accenture's technology and analytics capabilities and create a powerful investigation support tool that help identify suspicious transactions, understand links between risky entities, and raise Red Flags faster and more accurately.

- Suspicious behaviour
- Prioritise investigation
- Discovering new typologies
- Improve screening
- Red flags

accentureoperations

COMPLIANCE AS A SERVICE (CAAS)

Runs compliance remediation and BAU as a service (e.g. KYC, AML investigations, FATCA, client data / outreach, restructuring, exits and repapering).

- KYC Remediation
- Client Lifecycle Management
- Transaction Monitoring
- Regulatory Remediation
- Customer Restructuring & Remediation

OUR PRACTICE

Over 1,100 people globally with Financial Crime skills

Specialists with extensive knowledge of KYC, AML, Fraud, and Sanctions Compliance Programmes and Operating Models

Analytics Centre of Excellence for Financial Crime in Dublin

Onshore Operations Centre of Excellence in Newcastle

Offshore Operations capability in India and China

Global consulting experience

DEEP CAPABILITIES AND SKILLS

Know Your Customer (KYC)

Sanctions / List Screening

Transaction Monitoring and Investigations

Operating Model and Governance

Policy, Procedures and Internal Controls

Talent Management and Learning

Managed Services and Operations

Fraud & Financial Crime Analytics

Accenture is uniquely positioned to support financial institutions in their Financial Crime Compliance journey. Our strategic compliance framework is supported by our industry-leading expertise, assets and experience to achieve the best outcomes. Our mission is to future-proof our clients' operations, so that they can confidently navigate regulatory demand.

OUR STRATEGIC COMPLIANCE OPERATIONS CENTRES ACROSS THE GLOBE:

Here's a look at the journey from remediation to managed service:

REMEDIATION

Addressing immediate compliance needs and meeting imminent deadlines, by scaling quickly, providing flexible technology solutions and global capability, and servicing diverse language and complexity requirements

BOLSTERING THE BUSINESS

Incrementally using our technology ecosystem, process transformation expertise and diverse compliance offerings to address our clients' regulatory needs

MANAGED SERVICES

Delivering end-to-end compliance operations for our clients from our Accenture delivery centres; employing our analytics, consulting and technology partnerships to further develop and future-proof our clients' compliance operations

TOOLS & ASSETS

Accenture has invested in next-generation thinking, tools and assets that can help accelerate your compliance journey

PEOPLE

Accenture's blended workforce capabilities and skills means we can provide expertise across an array of services, spanning globally

Strategic Compliance Framework

PARTNERSHIPS

Accenture has developed alliances and partnerships with leading vendors, which enables us to deliver at pace

CREDENTIALS

Accenture is helping clients with financial crime compliance across multiple geographies, giving us unparalleled experience, and insights into industry and market trends

Authors

Ritesh Mazumder
Risk and Compliance SME,
Advanced Technology Centre, India
ritesh.mazumder@accenture.com

Tamal Das
Risk and Compliance Practice Lead,
Advanced Technology Centre, India
tamal.das@accenture.com

Devan Ayadurai
Finance and Risk Analytics CoE Lead,
Singapore
devan.ayadurai@accenture.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialised skills across more than 40 industries and all business functions — underpinned by the world's largest delivery network — Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.