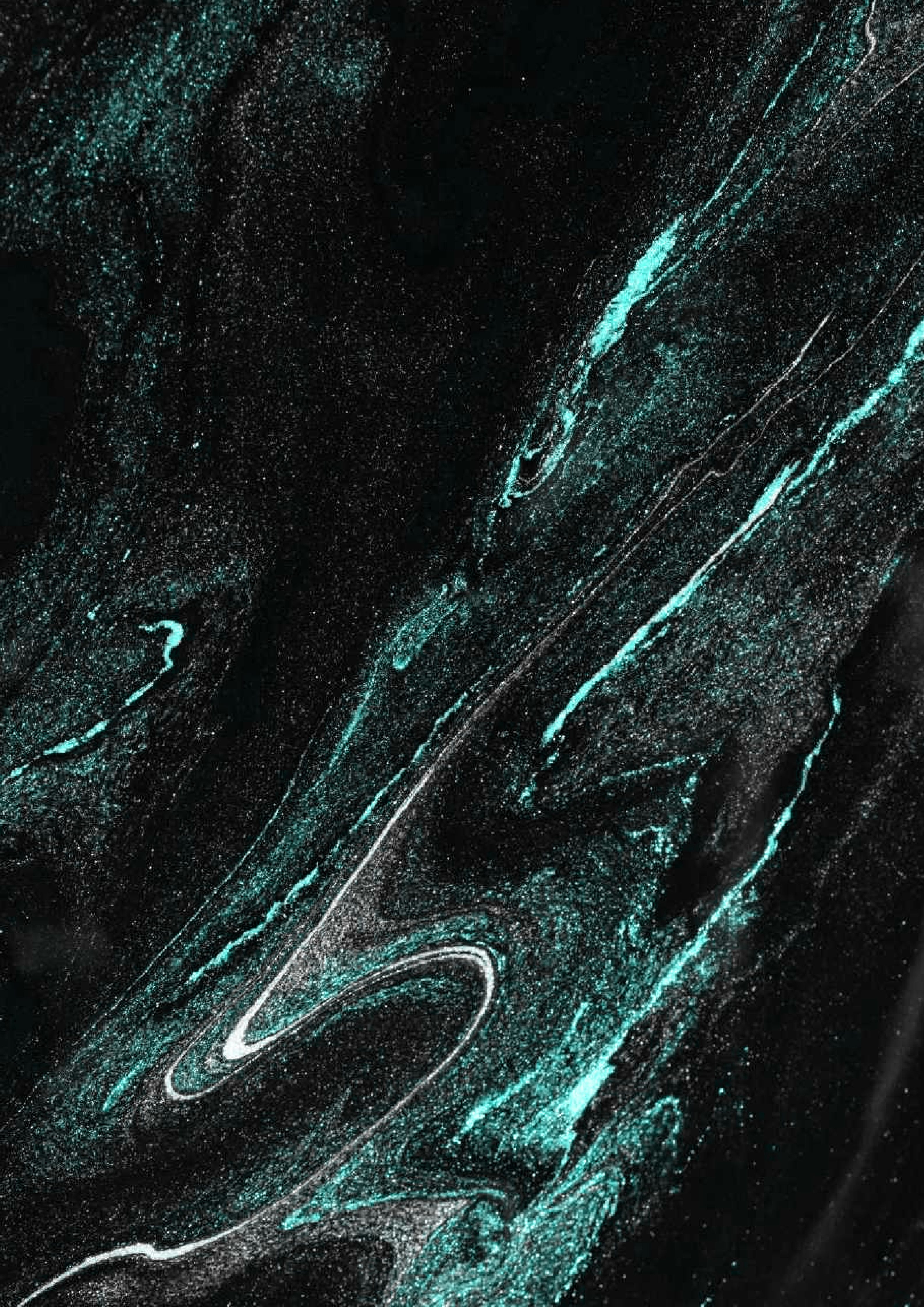
منتدى الشراكة في مواجهة غسل الأموال
وتمويل الإرهاب
AML/CFT Partnership Forum

المكتب التنفيذي لمواجهة غسل
الأموال وتمويل الإرهاب
EXECUTIVE OFFICE OF ANTI-MONEY LAUNDERING
AND COUNTER TERRORISM FINANCING

Current Views on Technologies in Anti-Financial Crime

White Paper – Summaries and Expert Commentary

Digital Working Group



This document offers a high-level overview of latest technologies that has proven to be or demonstrates encouraging possibilities in significantly improving capabilities to fight financial crime. The document caters to a wide universe of stakeholders covering Financial Institutions, Technology providers, Compliance / AML / Regulatory Technology professionals and anyone interested in the Anti-Financial Crime arena. The document has been developed by the Digital Working Group of the AML/CFT Partnership Forum, a Public-Private Partnership platform set up under the Executive Office of the Anti Money Laundering and and Counter Terrorism Financing in the United Arab Emirates. The Working Group has drawn on the combined experience of more than 50 leading professionals in the Anti Financial Crime field regionally as well as globally.

Contents

Foreword – Mohamed Shalo, Chair, UAE AML / CFT Partnership Forum 5
Introduction – Nishanth Nottath, Chair, Digital Working Group 7
Executive Summary 8
List of Contributors 11
DWG Members – Editing Team 11
Section contributors 12
Core contributors 12

Section A - KYC, CDD, Onboarding 15
Introduction 16
A new approach 17
The pKYC value proposition 18
Approach to Perpetual KYC 19
Key considerations 20
A bespoke approach 21
Development of effective rules 22
The importance of making space for innovation 22
Challenges in implementing pKYC 23
pKYC - Conclusion 23
KYC-Tech and the importance of Middleware – A PSP FinTech perspective 24

Section B – Transaction Monitoring and Surveillance 27
Introduction 28
Challenges 28
Adoption of automation and machine learning capabilities 29
Implementation of Holistic / Dynamic Risk Assessment (DRA) model 29
Master models 30
Single customer view 31
Leverage more non-traditional, non-transactional data sets 32
Use of Large Language Models 32
The evolution of technology 33
Use cases 33
Entity resolution 33
Behavioural Customer segmentation 33
Dynamic customer risk scoring (similar to Holistic Monitoring / DRA) 34
Event risk scoring 35
Thematic analysis 35
Network analysis 35
Natural language processing 35

Section C - Screening 37
Introduction 38
Legal and Regulatory Framework 39
Emerging Technologies 39
Challenges 39
Robotic process automation 40
Centralized Screening Utility 41
Centralised solution 42
Potential challenges 42
Roadmap 42
Conclusion 43

Section D : Model Risk Management / Data 45
Model Risk Management Framework 46
Use of emerging technologies in MRM 48
Data Quality Management Framework 49
Responsible AI - Overview 49
Use of technology – Responsible AI 50
Use of emerging technologies in DQMF 50
Challenges 50

Section E: Large Language Models 53
Introduction 54
Potential Use Cases of LLMs in Anti Financial Crime, KYC and Screening 54
Important Architecture elements to consider for LLMs 55
Pros and cons of an LLM infrastructure / architecture 56
Standard Steps for a PoC 57
Additional considerations 58
LLM PoC in AML use-case 58
Stage 1: Setting objective and outcome 58
Stage 2: Ideation 59
Stage 3: Planning key steps 59
Stage 4: Execution of key steps 60
Key Libraries used 61
Conclusion 61

Section F: Core Models – EWRA / FCRA, CRRM 63
Introduction 64
Technology landscape 65
Conclusion 65

Section G: Virtual Assets 67
Virtual Assets 68
Technology vs regulatory oversight 68
Legacy approach to technology 69
Privacy preserving technology 70
Looking ahead 70

Section H: Conclusion 71
Future Anti Financial Crime model and skills 73

Appendix 74
Appendix 1: pKYC risk drivers, sub-categories 74

Foreword

Mohamed Shalo

Chair, UAE AML / CFT Partnership Forum

There is no doubting today the pivotal role of cutting-edge technologies in the ongoing battle against financial crime. When I was appointed Chairman of the UAE’s AML/CFT Partnership Forum an early priority was the establishment of a dedicated working group focused on new technologies and their powers to help detect and prevent financial crimes. I am delighted that this initiative is spearheaded by the private sector and making important strides forward.

We are living in an era marked by massive technological advances that are fostering economic growth and driving innovation in the financial services industry. Increased efficiency, faster transaction times, and new solutions are combining to create unprecedented value. According to McKinsey, generative AI alone could create an additional $200 billion to $340 billion annually for the banking industry.

It is however a truism that opportunities of this scale attract the good (investors) but also the bad (criminals). Whether these criminals are seeking to abuse the new architecture of the global financial system to create ill-gotten gains, or simply defraud people and organisations, we know all too well that their crimes are one of the most significant systemic risks to the global economy today.

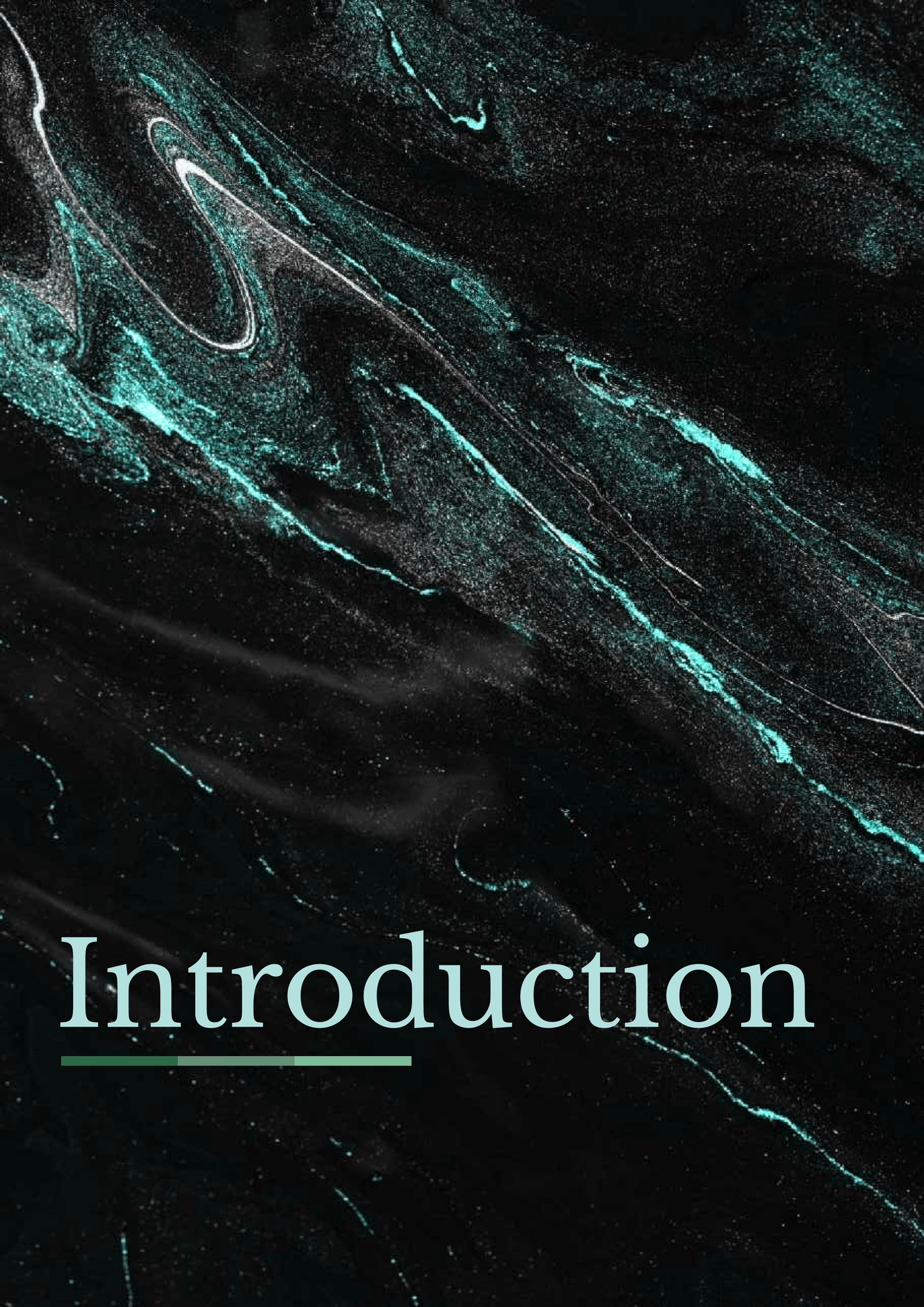
The staggering annual cost associated with money laundering and related crimes ranges from US$1.4 trillion to US$3.5 trillion according to a 2020 report by ACCA and EY. For financial institutions, the cost of fighting financial crime was US$181 billion globally in 2019 - an estimated three percent of revenues - according to Lexis Nexis Risk Solutions.

The good news is that new technologies, and in particular those developed by fintech and regtech sectors, can help to mitigate financial crimes risks. Key components in the private sector's arsenal against financial crime are the Know Your Customer (KYC) and anti-money laundering (AML) transaction monitoring compliance processes. These critical tools, however, hinge on access to high-quality data concerning customer accounts, products, and transactions. They rely too on human capital and the skillsets required to effectively leverage the new tools at our disposal.

What’s more, with the advance of technology comes a shifting of the financial crime landscape. To keep pace with criminals and detect and prevent their evolving activities, I urge the private sector to continue to invest substantially in R&D in this field. The UAE is home to several tech incubators and a dynamic VC community that positions the country very favourably for the opportunities that entrepreneurs are chasing.

The Digital Working Group demonstrates that both public and private sector institutions in the UAE are committed to combating financial crime and are striving to harness the power of the right technologies. By leading by example they demonstrate that organizations which embrace innovative technologies and work collaboratively are more than able to meet the challenges posed by tech-driven financial crime.

I would like to thank the members of the Digital Working Group and all who have contributed to this paper. As a stronger believer in role of strategic communication, I can attest to the power of collaboration and the sharing of expertise. I recommend this paper to experts from all sectors, including the academic community; its contents and recommendations will be of real value to those at the front line of the fight against financial crime.



Introduction

Nishanth Nottath

Chair, Digital Working Group

It has been my great privilege to be called upon by the UAE AML / CFT Partnership Forum (previously titled UAE Public Private Partnership Committee) to form a Working Group to foster spirited discussions and dissemination of original thought related to the use of Technology in supporting fighting financial crime. The Digital Working Group was formed in Q3 2022 with 8 leading industry practitioners joining hands to start deliberations in a structured manner.

Following extensive discussions and consultation, the Working Group decided to write a White Paper covering the latest thoughts on technologies in fighting financial crime. We reached out to a large number of Compliance leaders and leading practitioners in Anti Financial Crime (AFC) technologies and our efforts have been enriched beyond all initial expectations with enthusiastic collaboration from c.45 regional and global experts in the field.

We stand at the cross-roads of breakout technologies. The last decade has witnessed a general disruption of the Financial Services industry with a technology-fuelled ecosystem, where increasingly non-traditional players are making significant inroads in the business of storing and transferring value (beyond the concept of just money) faster than the blink of an eye, globally. Whilst speed and customer experience has catapulted, the entire ecosystem is increasingly fragmented, introducing additional layers and reduction in transparency.

However, on the other hand, we are witnessing the emergence of technologies such as Generative AI and Large Language Models (LLM). With breakthroughs in processing speeds (GPUs), increasing availability of Cloud ecosystem, we are witnessing unprecedented pace in adoption of tech, advanced analytics and models in the AFC arena. Leading global companies are investing billions in the next frontiers of technology – Quantum computing and Artificial General Intelligence (AGI). Setting aside the debate on the philosophy of AGI or the profound impact on humanity, it is critical that AFC practitioners keep a close tab on emerging tech as these will have a direct impact on their work. Criminals are always on the look-out for better ways to obfuscate their trails of crime. We should remain at the forefront, and the mission will only be successful if we remain up to-date and master these technologies.

The day is not far where financial crime analysts will increasingly interact with vast amounts of data at their disposal through LLM or LLM-style interfaces. One leading Middle East Bank has already delivered a proof of concept (PoC) where analyst is able ask questions through the prompt and get answers in an almost conversational manner and there is no doubt that such capabilities will have profound impact in the way we work in future. The paper covers all the key pillars of controls and associated leading technologies –the move to perpetual KYC, adoption of holistic / dynamic risk assessment models for ongoing surveillance, the emergence of centralised screening utilities, promise of Generative AI, use cases and a road-map for executing a PoC, the importance of effective model risk management in the context of increasingly complex models at play, and the ethical considerations in adopting AI at almost all parts of the business and control framework and of course, latest thoughts on AFC controls in the space of Digital / Virtual Assets. With higher powers, comes higher responsibilities – there is a need to rethink the way AFC frameworks are designed and executed. With scaling of digital financial services and products at break-neck speed, throwing more human resources and reliance on detective controls is no longer sustainable or effective in the long run. The core design language of the control framework for a digital business needs to shift to a 'Compliance in design' principle. Well designed preventive controls help scale products and services faster and safer.

For sustainable change, however, a shift in mindset as well as skill-set is necessary, to build a future-ready Compliance / AFC programme. The last parts of the paper explore a potential roadmap to rethink organisational design to achieve core and complementary skills – for Risk Analysts and Risk Engineers.

These are exciting, once in a generation time for AFC professionals to forge ahead and be at the forefront of fighting financial crime, aided by cutting edge technology. I wish all the readers every success in this journey to make the world a safer place.

Executive Summary

Over the last 50 years, the financial sector and the commercial environment have experienced profound change. Whilst globalisation and technological innovation have brought incredible benefits for some, it has also allowed bad actors to move funds around the world with ease, evading detection and accountability. The increasing volume of illicit financial flow adds to global inequality, threatens democracies, robs developing economies of much-needed tax revenue, and erodes trust in the financial system's integrity.

Over the years, authorities have increasingly turned to banks and the private sector to police and protect the financial system. Compliance obligations have grown substantially, with some arguing the cost of compliance now outweighs the outcome. A recent study, for example, estimates financial crime compliance costs for UK financial services to be GBP34.2 billion per annum, a significant increase of 19% from a previous study conducted two years prior. Yet it is suggested that only 1% of the illicit financial flow is detected.

A cost squeeze is understandable; compliance teams and AFC professionals are asked to do more with less. Unsurprisingly, sophisticated and innovative technology has become so much of a focus. We asked several regional and global thought leaders and experts in the compliance field for their opinions on recent technology developments and summarised their insights in this White Paper. We dissect various aspects of technology implementation over five chapters; each section explores key elements of the compliance challenge, from Know Your Customer (KYC), Customer Due Diligence (CDD), and onboarding to Transaction Monitoring and Surveillance, Screening, Model Risk Management/Data, and the transformative influence of Large Language Models (LLMs).

KYC, CDD, Onboarding

The KYC process is one of the more essential elements of the compliance process, and it plays a vital role in the relationship between an organisation and its customers. The process is plagued with inefficiencies, causing delays, and absorbing substantial resources.

Our experts underscore the need to move beyond periodic reviews, improve accuracy, and streamline the process. The shift towards digital transformation is not merely an option but necessary for ensuring efficacy and customer satisfaction.

Transaction Monitoring and Surveillance

Transaction monitoring and surveillance processes, critical for identifying and preventing financial crimes, are challenged by the diversification of financial services and emerging payment methods. Traditional models struggle to keep pace with the dynamic nature of financial transactions, necessitating a paradigm shift in understanding typologies and red flags. Our experts explain an urgent need to re-evaluate existing systems and update standards in a rapidly changing regulatory and risk environment and call on regulators to ensure they stay up-to-date.

Screening

As a critical primary control mechanism, screening remains fundamental in AML/CFT frameworks. This chapter explores the complexities of name screening, emphasising the importance of considering variations in spelling and transliterations. Transaction screening, a parallel process, employs advanced software systems but grapples with challenges from fragmented transaction flows. Our experts emphasise the need for continuous vigilance and technology adaptation to counter risks effectively.

Model Risk Management / Data

Financial institutions heavily rely on models for decision-making, introducing inherent risks.
The Model Risk Management Framework (MRMF) becomes a crucial tool in identifying, assessing, and managing these risks. The report highlights the critical components of a robust MRMF, emphasising the importance of collaboration between compliance professionals and independent model review teams. The dynamic nature of financial crime regulation requires adaptability in both technological solutions and the associated risk management processes.

Large Language Models

Large Language Models (LLMs) have emerged as powerful tools, particularly in KYC and screening processes. The potential use cases of LLMs, including fraud detection, reflect a paradigm shift in leveraging advanced technologies. However, integrating Generative Artificial Intelligence (gen AI) introduces ethical and operational considerations, underlining the importance of balancing automation and human expertise.

Core Models – EWRA / FCRA, CRRM

Addressing the pervasive threats of money laundering and terrorist financing necessitates a comprehensive approach, beginning with an enterprise-wide risk assessment (EWRA). This chapter outlines the critical steps in conducting an effective EWRA, emphasizing the importance of risk assessment frameworks, identifying and assessing risks, and implementing robust mitigation measures. Obstacles to implementing a sound solution include data availability, resource constraints, evolving regulatory environments, and transparency issues. The section describes the slower pace of technological development in EWRA compared to other areas like KYC and transaction monitoring. It explores opportunities for progress, particularly in automating data collection, creating interactive reporting dashboards, and leveraging blockchain for transparent recordkeeping.

Virtual Assets

This chapter discusses the inherent challenge of synchronising technological development with regulatory evolution. While virtual assets hold promise for financial crime detection, experts point out the lag in regulatory oversight.
The potential integration of blockchain analytics with traditional financial crime technology is explored, focusing on the growth in conventional finance organizations managing exposure to virtual assets.

Final thoughts
The convergence of technology and anti-financial crime is at a critical juncture, and a comprehensive and adaptive approach is needed to navigate a quickly evolving landscape. *"A FC professional of the future (I would say that it is a need of today) needs to be well versed with emerging / emerged technologies that are driving change and disruption to seasoned systems and processes as technology is evolving rapidly, introducing greater opportunities but also greater risks. There is a need to enhance the way AFC professionals are trained and upskilled. They will likely need to be multi-skilled with in-depth knowledge of the enabling technologies in financial sector and those in the financial crime detection and prevention space, internal and external data sources, models, data ethics, data use and analytics and of course the Regulations themselves. AFC professionals will be augmented by Tech, including AI and potentially AGI – however, I believe that there will still be a need to have an AFC professional opine on what the tech platforms produce albeit it will become more efficient and resolve some of the challenges we have struggled with for example unmanageable false positive alert numbers and the like."* Reflects **Collin Lobo**, Regional Head of Financial Crime Compliance & MLRO, HSBC MENAT.

Whether through digital transformation in KYC, redefining transaction monitoring, enhancing screening capabilities, implementing robust model risk management, or integrating LLMs, financial institutions must embrace innovation to stay ahead of financial criminals. We are only beginning this journey, and decision-making can be challenging in this environment. This report is a snapshot of the progress and value of technology in the compliance field.

Victor Matafonov, Group Head of Compliance at EmiratesNBD reflects,

"The use of technology and advanced analytics to fight financial crime continues to be a significant priority for banks worldwide. The use of manual or tactical solutions to address new regulatory requirements or to rectify prior weaknesses is not sustainable from a regulatory or financial perspective. Therefore it is critical for FIs to continue investing in technology solutions across all lines of defense to better identify illicit activity more efficiently".

List of Contributors

DWG Members – Editing Team

BHAVIN SHAH
Managing Director,
Secretariat Advisors

DR YOONUS C. AHAMMED
Director, FCSO TM Analytics,
OPS FCSO Transaction Monitoring,
Standard Chartered Bank

DAVID SHEPHERD
Global Head,
Customer Risk Proposition,
Risk Intelligence,
London Stock Exchange Group

MUZAMMIL EBRAHIM
Partner, Financial Crime
and Analytics Leader,
Deloitte

NIPUN SRIVASTAVA
Managing Director,
Financial Services,
Protiviti

NISHANTH NOTTATH
Executive VP, Head AML,
ABC and RegTech,
Mashreq Bank

SAMEER KUVVAKKATTAYIL
Executive Head, Financial
Crime Compliance and
Group MLRO, Group
Compliance,
Abu Dhabi Commercial Bank

WAI LUM KWOK
Senior Executive Director -
Authorisation & Fintech,
Financial Services Regulatory
Authority

Section contributors

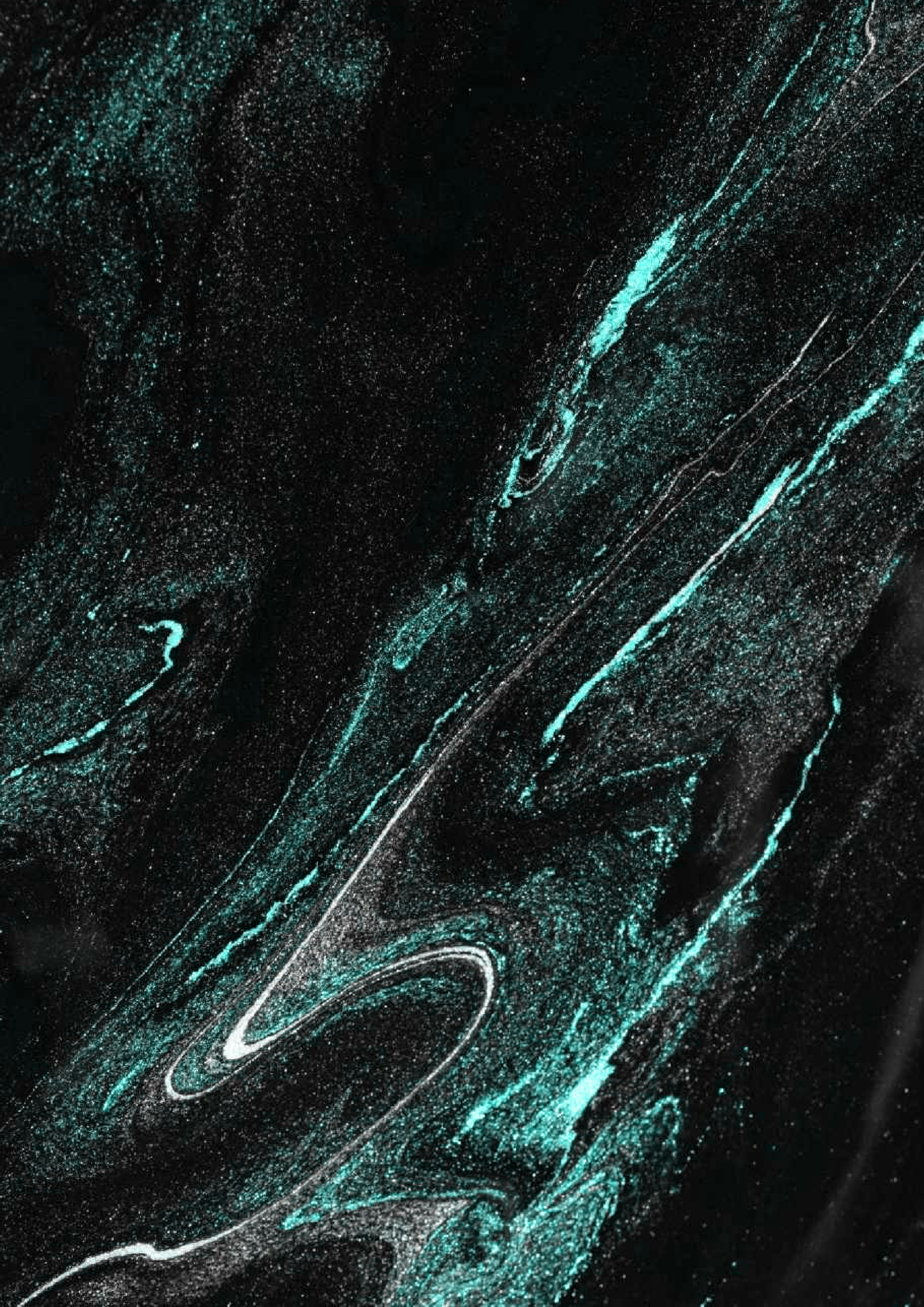
Section	Name	Designation
KYC and importance of Middleware	Javier Pimentel	Head of Compliance MEA, Amazon
Centralised screening utility	Praveen Jain	Head of Client Success at GSS – Global Screening Services
LLM	Prashant Chauhan	Head, Data, Platform and Analytics, Compliance, Mashreq Bank
	Vinod Viswanathan	Head, Investigations and RRU, AML Compliance, Mashreq Bank
	Imran Khan Anwer Neelufer	Director AI & Data, Deloitte
	Charmian Simmons	Financial Crime and Compliance Expert, Sensa-NetReveal
	Eve Whittaker	Business Solutions Consultant - Financial Crimes, Sensa-NetReveal
	Peter Bove	Sales Executive, Sensa-NetReveal
EWRA	Nicki Koller	Manager Financial Crime & Analytics, Deloitte
Screening	Multiple individuals	Team at Forensic Risk Alliance

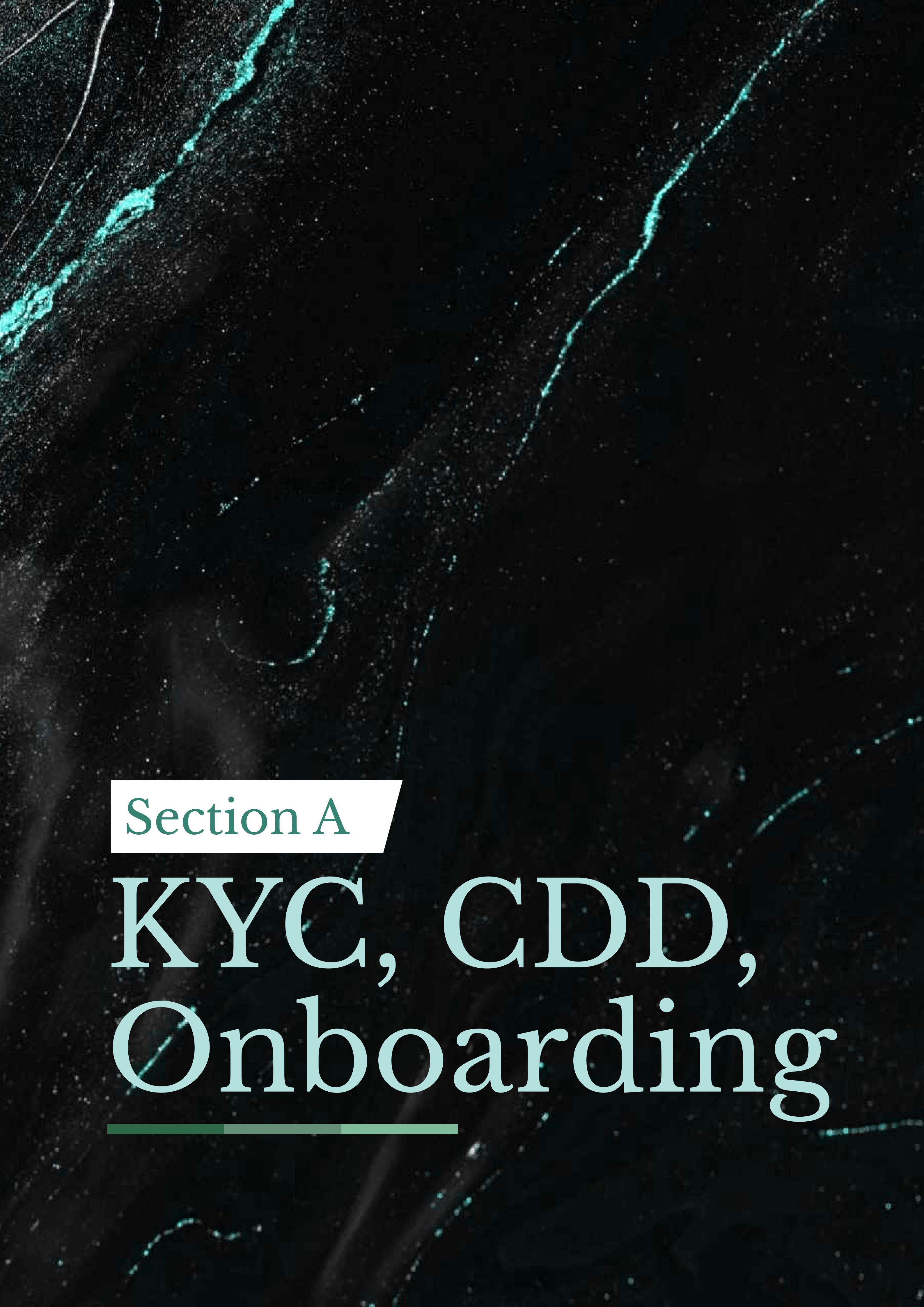
Core contributors

Name	Designation
Adnan Malik	Head of Conduct, Financial Crime and Compliance Advisory, Standard Chartered Bank
Amit Sharma	Chief Executive Officer, Finclusive
Asaf Meir	Chief Executive Officer, Solidus Labs
Collin Lobo	Regional Head of Financial Crime Compliance, MENAT, HSBC Middle East
David Carlisle	Vice President of Policy and Regulatory Affairs of Elliptic
David Choi	Partner, Oliver Wyman, US
David Howes	Global Head, Financial Crime Compliance, Conduct & Compliance Framework, Standard Chartered

Core contributors

Name	Designation
Haibo Zhang	Fintech / Regtech Consultant, Founder, Compliance Analytics UK
Hassan Gulamali & Dee-Ann Chick	Financial Crime Business Oversight Compliance, Barclays
Heather Adams	Managing Director, Head of Risk & Strategy Consulting, Accenture
Jas Randhawa	Founder and Managing Partner of StrategyBRIX
Jonathan Falconer	Head of Compliance, National Bank of Fujairah
John Cusack	Chair, Global Coalition to Fight Financial Crime
Marcus Lau	Group Financial Crime Compliance, Oversea-Chinese Banking Corporation
Mark Newfield	Senior Vice President, Head of Compliance Systems, Emirates NBD
Matthew Hobbs	Head of FCC Strategy and SSP, SWIFT
Michael Mosier	Co founder, Arktouros and former Acting Director at FinCEN
Neil Thomas	Head of Financial Crime Systems, Compliance, Commercial Bank of Dubai
Pascal Aerens	Co-Founder and CPO, Neterium
Paula Borges	Global Head of Financial Crime Controls, Stripe
Rasha Mortada	Group Chief Compliance Officer, Abu Dhabi Commercial Bank
Richard Hills	Senior Managing Director, Financial Crimes Compliance practice, K2 Integrity
Scott Ramsay	Group Chief Compliance Officer and Bank MLRO, Mashreq Bank
Scott Werner	Associate Partner, McKinsey & Company
Shameek Kundu	Head Of Financial Services and Chief Strategy Officer, Truera
Swagatam Sen	Executive Director, Compliance Tech Advisory, Santander
Victor Matafonov	Group Head of Compliance, EmiratesNBD
Zubin Chichgar	Group Head of Compliance Operations at EmiratesNBD
Dr Samoj Panicker	Head, Compliance Surveillance Data and Analytics, Standard Chartered Bank
Estaban Castano	Chief Executive Officer, TRM Labs





Section A

KYC, CDD, Onboarding

Introduction

Know Your Customer (KYC) protocols are essential elements of successful risk and compliance programmes. Financial institutions need to know who is doing business with them, which is why the KYC process is critical to identify any red flags or risks associated with new and existing customers. KYC cannot be a one-and-done process at the time of on boarding. Regulations now require financial institutions to review customer data periodically throughout the relationship. The schedule of periodic review is at the organisation's discretion and depends on risk appetite and resources.

While essential, the KYC process can be time-consuming, laborious and beset with challenges. KYC documentation can vary significantly between jurisdictions and is sometimes difficult to source, often subject to language barriers, unavailability of golden sources, bureaucratic bottlenecks and archival challenges. The process of customer risk assessment and risk re-categorisation can also be impacted by manual processes and data silos. It is not surprising that many customers report a negative experience: a recent survey shows that 68% of consumers have abandoned an application for a financial service in the past year, 21% say it takes too long, and another 21% are asked for too much personal information.[1]

Ironically, the majority of customers pose very little risk, yet so much of the organisation's compliance resources are diverted to this purpose. Typically, high risk customers are reviewed each year and medium and low risk customers every three and five years respectively.

> *"Overall, the current time-based periodic review model is past its shelf-life. In one case working with a major FI, we reviewed approximately one million customer records and saw many changes of Critical Data Elements. But, when we ran a data analysis, we found that these changes did not affect 94% of the reviews. The risk rating stayed the same or went down. A lot of the noise came from a simple address change, for example"*, notes **Heather Adams**, Managing Director at Accenture.

[1] How to avoid flunking your customers' onboarding experience, Refinitiv, July 3 2023

A new approach

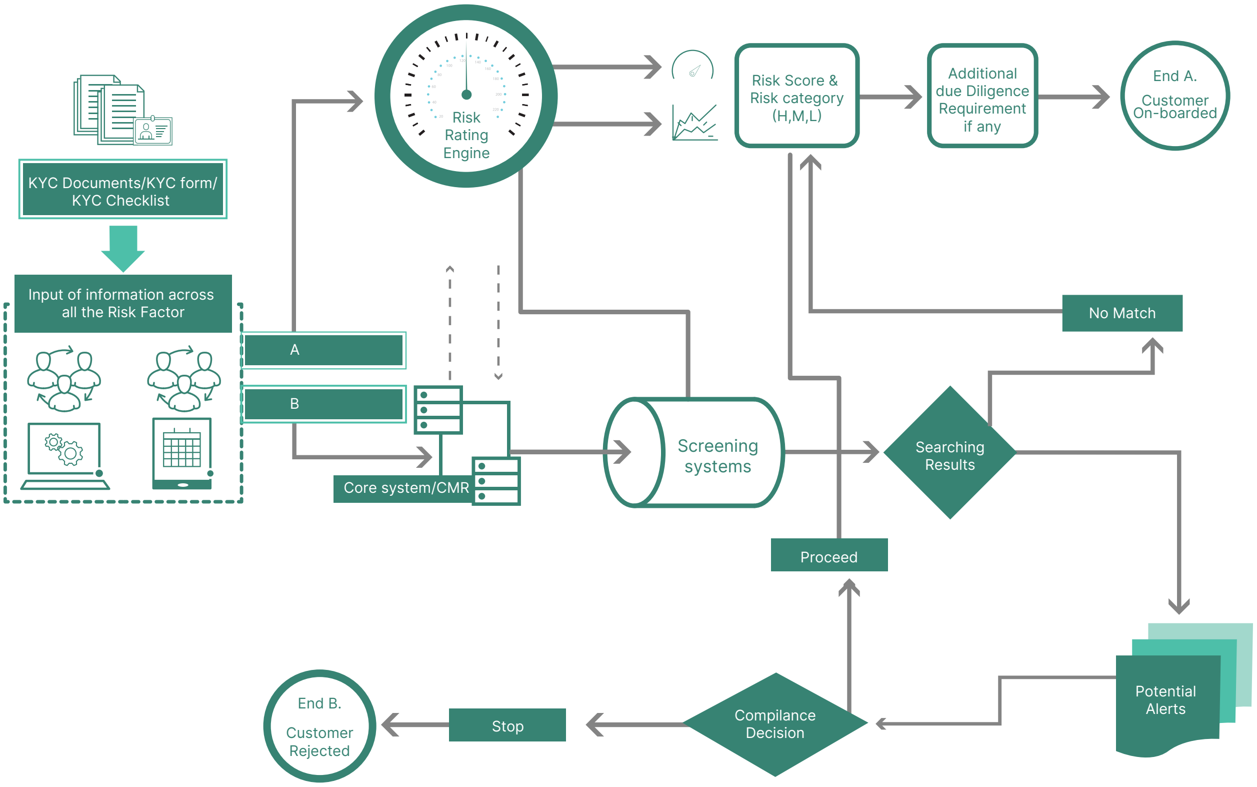
We are in the midst of digital finance evolution, where most customers are on-boarded digitally and banking online or using digital platforms, managing their money in an exponentially high speed with a few taps on a screen, changing how financial institutions do business. Evolving technology also means financial institutions need to evolve the methods through which they conduct KYC and customer risk assessment.

The last few years have seen a transformation in the way financial institutions approach KYC requirements. With the increase in regulatory pressure to ensure that financial institutions are keeping compliant with AML/CFT regulations and implement a robust anti-financial crime control framework, a move from the traditional periodic reviews to Perpetual or dynamic KYC review is increasingly moving from aspirational to expectation.

Perpetual KYC (pKYC) involves a more sophisticated data analytics to ensure a comprehensive customer risk assessment, utilising Artificial Intelligence and Machine Learning tools, whereby customers are risk re-assessed based on their increased probability to commit a financial crime.

The time lapse between scheduled reviews exposes financial institutions to the risk of financial crime, reputational damage and regulatory fines, whereas the perpetual KYC significantly shortens the window in which criminals can act.

Perpetual KYC is Risk Based Approach and has the potential to meet most of the challenges posed by the traditional periodic reviews.



KYC Documents/KYC form/ KYC Checklist
Input of information across all the Risk Factor
A
B
Core system/CMR
Risk Rating Engine
Risk Score & Risk category (H,M,L)
Additional due Diligence Requirement if any
End A. Customer On-boarded
Screening systems
Searching Results
No Match
Proceed
Potential Alerts
Compliance Decision
Stop
End B. Customer Rejected

Source: Protiviti Consulting

The pKYC value proposition

pKYC is the continuous monitoring of customer behaviour as a whole, leveraging on automation and statistical models. A mature pKYC process, if supported by the right infrastructure, could even automatically re-verify existing identity documentation, reducing time and resource cost, and escalating new risk events for the analyst to consider. By adopting a perpetual KYC approach, financial institutions can move towards preventive, and perhaps even predictive, financial crime controls. pKYC offers several advantages over the traditional model.

- **Improved compliance risk management and resource allocation**

  By analysing static and dynamic data such as transaction history, financial statements, digital foot-print / behaviour through digital channels, meta-data and publicly available information, financial institutions can better understand customer behaviour and assess their risk levels, thereby enabling financial institutions to carry out appropriate KYC, customer due diligence (CDD), and enhanced due diligence (EDD) measures to identify high-risk customers. pKYC allows organisations to view their financial crime risk exposure with a higher degree of accuracy and time relevance, help improve risk management standards and achieve a more precise categorisation of customer profiles.

- **Improved efficiency and reduction in fraud**

  An improved customer risk categorisation process enables a more efficient and effective resource allocationpotentially helping achieve long term savings (in some cases of almost 60-80% in related costs[2]). In addition, withalmost one in ten account creations in the Middle East affected by identity fraud attack[3] , FIs are better equipped to quickly isolate high-risk accounts and limit the damage.

- **Risk-based response**

  pKYC programmes coupled with risk-based monitoring[4] of customer activity and profile changes can support FIs in investigating and reporting suspicious activities of customersdeploying a ‘higher-risk-events-first’ approach more effectively instead of the traditional approach.

  Indeed, the clever use of technology can make a huge impact, notes **David Howes**, Global Head, Financial Crime Compliance, Conduct & Compliance Framework, Standard Chartered: *“There is a lot of opportunity to automate what large teams do, to improve the speed at which humans work through technology.”*

- **Real-time decision making**

  Institutions can review and update customer information continually rather than wait for the periodic review due date or trigger event, enabling appropriate actions in real-time. Such actions may include updating customer risk profiles, carrying out additional due diligence, applying enhanced transaction monitoring and restricting access to certain services.

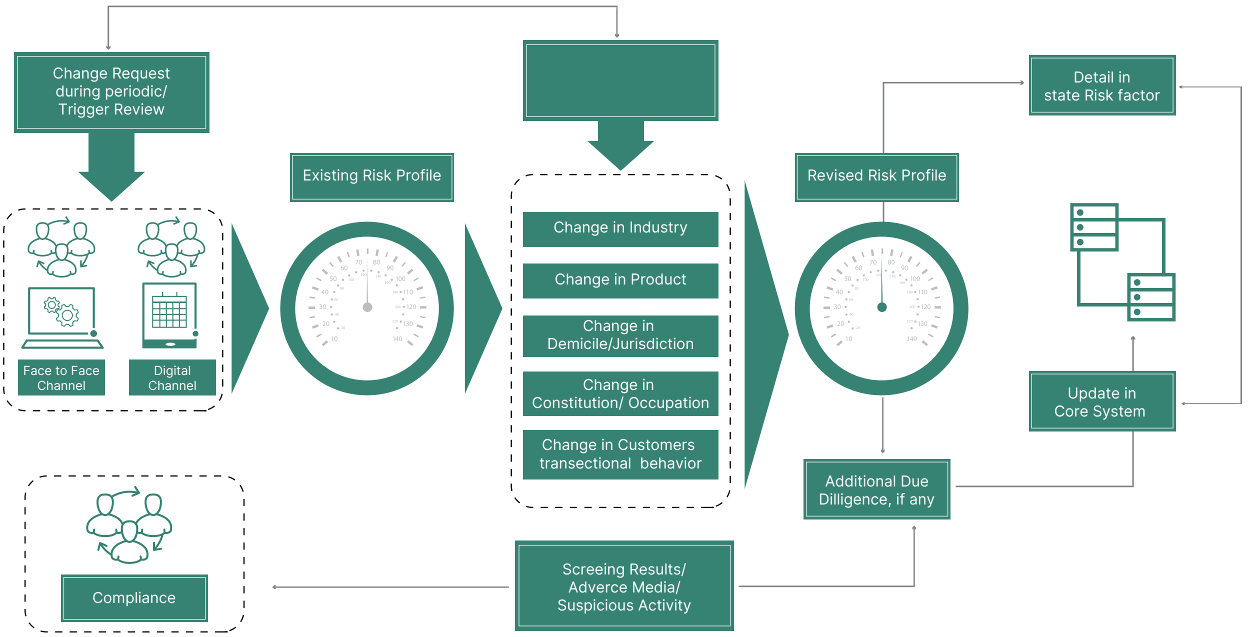
- **Enhanced data quality, regulatory compliance and customer experience**

  Balancing regulatory compliance with a premium customer experience can be challenging. Detailed verification requirements or repeated requests for information can lead to frustration and poor customer experience. With pKYC, businesses can streamline customer onboarding and verification process by drawing on alternative data sources such as national identity databases, eKYC and face recognition databases, corporate registries, and tax databases, eliminating the need for repeated identity verification, reducing burden on customers. The ability to draw on other data sources can also help future proof the compliance function against evolving regulatory demands.

[2] Multiple industry studies, average estimates | [3] LexisNexis, industry sources | [4] There is no suggestion that all monitoring capabilities are recommended to be real or near real-time; rather, deploying a risk-based approach, those typologies or highest risk activity that warrants swift risk management action may be prioritised

Approach to Perpetual KYC

pKYC uses automation and feeds from a many sources to better understand the customer's behaviour, at any point in time automatically, assign scores, leaving only a few actions to be performed manually. It allows the FIs to look beyond customer ratings assigned at the time of onboarding and get a real-time view of the customer from a ML / TF and sanctions risks perspective.


Change Request during periodic/ Trigger Review
Face to Face Channel
Digital Channel
Existing Risk Profile
Change in Industry
Change in Product
Change in Demicile/Jurisdiction
Change in Constitution/ Occupation
Change in Customers transectional behavior
Revised Risk Profile
Detail in state Risk factor
Update in Core System
Additional Due Dilligence, if any
Screing Results/ Adverse Media/ Suspicious Activity
Compliance

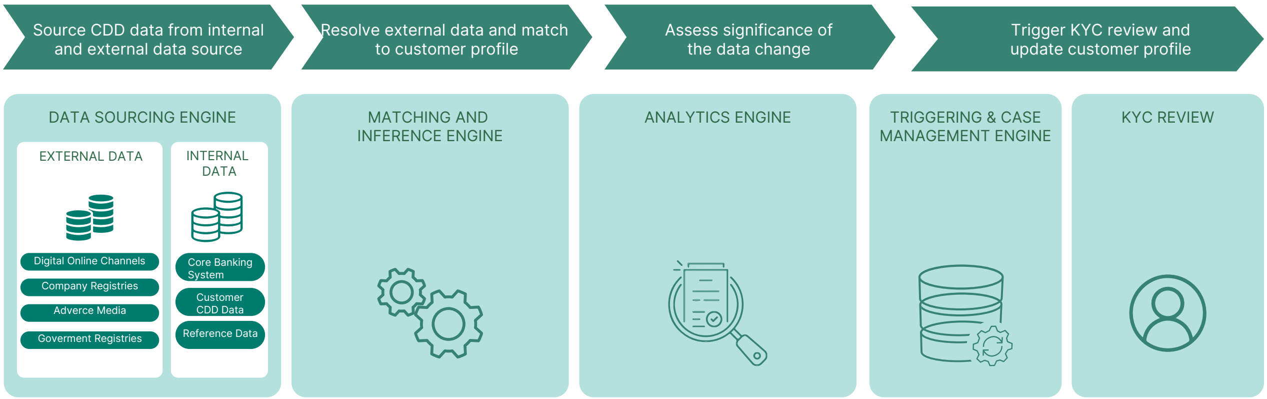
Source: Protiviti Consulting

At each step, the focus is on centralising and digitising back-end KYC compliance operations, keeping in mind specific business requirements and maintaining ongoing monitoring. Institutions can overlay these steps with functionality and limitations of their current channels, data feeds and core systems to ensure seamless integration of back-end and front-end systems for a successful transition to pKYC.

KYC value chain step	Business Requirement	Automation Consideration
Case assignment	Umbrella workflow	Business rule led outcomes
Document verification	Data aggregation KYC utility integration (multifactor authentication)	Data feedback led outcomes
Risk assessment	Risk calculator Data aggregation Behavioural fingerprinting	Business rule led outcomes
Screening	Threat identification Auto dispositioning of potential alerts	Business rule led outcomes Intelligence led outcomes
Client communication	Middleware bots Umbrella workflow	Data feedback led outcomes
Quality control	Middleware bots	Intelligence led outcomes
Approval & final decision	Umbrella workflow	Business rule led outcomes

Key considerations

pKYC is a technology-intensive programme. The use of API-connected networks in financial services, expected to expand significantly with the advent of Open Banking and Open Finance, will be a driving force behind the switch to pKYC. To gather data, including identity of Ultimate Beneficial Ownership (UBOs), and dissect corporate structures, CDD needs to access a variety of data sources. Previously, this could only be done manually but many FIs are now leveraging APIs to link their KYC systems to pertinent databases to automatically source information.



Source CDD data from internal and external data source

Resolve external data and match to customer profile

Assess significance of the data change

Trigger KYC review and update customer profile

DATA SOURCING ENGINE

EXTERNAL DATA

Digital Online Channels
Company Registries
Adverce Media
Goverment Registries

INTERNAL DATA

Core Banking System
Customer CDD Data
Reference Data

MATCHING AND INFERENCE ENGINE

ANALYTICS ENGINE

TRIGGERING & CASE MANAGEMENT ENGINE

KYC REVIEW

- Batch/API feeds to success all relevant data from internal and external data sources
- Data source and type will vary according to customer and geography
- Where data is not available in public domain, alternative sources such as media and transactional information can be utilized

- Source data is clean and prioritised data from external source matched to customer or inferred using specific data point
- Continual entity resolution as new data becomes available and new customer Relationship are established
- Multiple source can be used to increaseconfidence level

- Analytical technics are used to significance of change to customer data and identify changes in risk posed in bank
- Built in rule can aggregate changes to provide a view of materiality based on customer risk profile

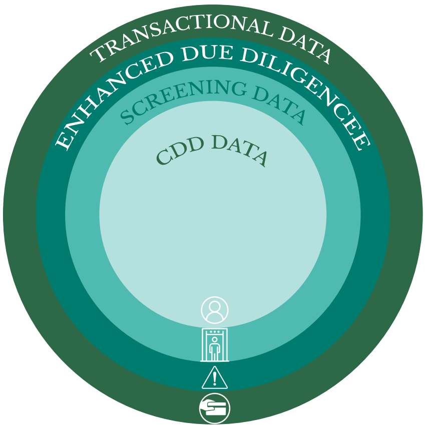
- Reviews are triggered based on material or admin change or risk events
- Automic data update, prioritisation of human reviews or automated customer contact request are generated based on nature of the change

Source: Protiviti Consulting

Currently, there are limited end-to-end solutions which can help FIs operationalise pKYC as plug and play. Creation of a flexible component-based architecture centred around a golden source of data is a critical first step to enable the transition to pKYC. Key attributes of component-based architecture include:

- Modular segregated services by business function / outcome
- Services available via micro-services and APIs
- Data-centric technology with data lineage at the core
- Common data model across functions
- Big data driven with a view to move to the cloud
- Core technology stack available for multiple use cases with information sharing across functions
- In-built and automatic feedback loops for model improvement
- Automated business processes and data collection
- Ability to integrate multiple vendors and solutions
- Entity resolution, single customer view
- Customer event and risk assessment models
- Customer screening and alert disposition
- Automated case generation
- Automated customer outreach
- Smart case allocation and workflow management

Controls required to prevent financial crimes, which rely on efficient and accurate data sourcing and monitoring



Capabillities which form the building blocks to achieve the end-to-end KYC solutions to combat financial crime

New capabillities for data driven KYC					Other KYC Capabillities			
Data sourcing and management	Entity resolution single customer view	Automated Research and data extraction	Customer event and risk assessment	Customer screening and disposition	Automated case generation	Automated customer outreach	Smart case allocation	Smart work flow and case management

Source: Accenture

A bespoke approach

pKYC does not mean a one-size-fits-all approach. The design of pKYC depends on the type pf customers, markets, lines of businesses, each requiring a different journey. Further, it is not that every customer shall be subject to only pKYC, rather, there will be customer types that must follow a trigger approach (over-riding pKYC), for example, Trusts, complex customers, correspondent banking etc.

Development of effective rules

Whilst a pKYC model must consider the specific business needs, context of products offered and digital channels or customer interaction protocols, the following set of risk drivers and behaviour rules can be considered for triggers in a pKYC model.

- Overall cash parameters
- Non-cash (except international wires) parameters
- Remittances parameters
- Overall account activities
- Other customer behavioural parameters
- Triggers for corporate customer
- Non transactional behaviours i.e. significant digital foot-print changes
- Inputs from non financial crime triggers (e.g. credit default)

For more details on sub-categories and description, refer [Appendix 1]. These risk factors are not meant to be used as transaction monitoring detection scenarios where substantial time is required for alert investigation. Instead, business rule-led analytics can be configured and automated for fast and efficient threat identification. Needless to say, technology data and operational enhancements are imperative to effective pKYC implementation.

The importance of making space for innovation

Implementing pKYC requires a new mindset from organisational leadership. **Swagatam Sen**, Executive Director, Compliance Tech Advisory, Santander, warns that the evolution of technology is fast and getting faster, but that internal governance at times is not agile enough to cope. *"Sometimes, the quest for 100% proof of success before committing to a three to five year investment hampers confidence to try and sometimes fail, and we need to change the game substantially here. Goal for the organisation is to be able to strike a balance between speed and assurance of success. One possible way is to allocate a designated space for innovation that allows safe experimenting with a differentiated risk appetite ring-fencing the risk exposure"*.

Other compliance experts pointed to the importance of senior leadership insight and understanding. **Richard Hills**, Senior Managing Director, K2 Integrity, believes that organisations fail to consider digital culture: *"Not everyone understands the importance of technology, especially at senior levels. Data-driven decision-making requires better data. This is a core issue."*

Innovation does not happen by chance. Ensuring that senior management and board members stay informed and supportive of efforts to transform the KYC function digitally will be key to the success of the project. Without senior management support, the adoption of new technology to help solve old problems will be slow. *"The future of financial crime risk management will increasingly revolve around the customer – as assessed through their persona and supported by better context – leading to effective scoring to help gain a unified view"*, reflects **Mr Howes**.

Mark Newfield, Senior Vice President, Head of Compliance Systems, Emirates NBD points to the UAE Pass app as an example of emerging technology that has experienced rapid adoption. To register for a basic account requires an Emirates ID card and face verification, and once registered, people can access the services of over 6000 government, semi-government and private sector agencies and organisations. *"Digital identity like UAE Pass has a lot of potential and can potentially be done on the blockchain"*, **Mr Newfield** points out. This digital identity method is already being used by several local FIs not only as an authentication method but also as a blockchain-based document sharing platform that serves to onboard new customers and facilitate KYC updates.

Challenges in implementing pKYC

Switching to pKYC is not without challenges:

- Poor KYC legacy data: To elicit the required alerts / triggers / insights for KYC refresh in line with pKYC standards

- Data and technical centralisation: Non-integrated systems and data sources in FIs that require significant technical investments to integrate the end-to-end workflows prevent seamless flow of information and implementation of pKYC standards

- Talent skills upgrade: pKYC requires a different approach to KYC refresh and staff requires re–training makers become checkers and controllers analysing data feeds from internal and external sources to decide on appropriate actions. In addition, new structures and profiles emerge requiring onboarding of new skill sets such as data scientists and automation experts within the team

- Alerts avalanche: With the implementation of pKYC, a high number of alerts, many times non-material, will be generated that require human interaction. Current teams may not be sufficiently equipped to handle such sudden workload increases, till such time sufficient experience is gained and models fine-tuned

- Customer friction: During the initial stage, there may be increased interactions between the FI staff and the customer impacting the overall experience and causing friction. However, this is short term, and as the process settles down, with increasingly more interaction through digital channels (e.g. mobile app, secure WhatsApp etc.) customers will appreciate the need for fewer interactions and the better experience driven by deeper real-time insights.

pKYC - Conclusion

pKYC is an evolving practice with no standardised model or solutions. It requires significant investments in transitioning from legacy systems, centralised data models and processes. With continued reliance on human agency, pKYC involves retraining staff to analyse trigger events in real-time and act accordingly, till fully automated reliable solutions emerge. Above all, pKYC requires an organisational mindset focused on maintaining updated KYC records, which is a radical change from the traditional approach.

Many FIs are realising the benefits of deep customer insights from updated KYC processes. These insights allow for a deeper engagement with their customers, helping to anticipate customer needs, improve the customer experience and increase retention, as well as reduce the incidence of fraud. As FIs embrace integrated IT platforms that connect customer relationship management, back-end systems with risk management and compliance monitoring, pKYC will become more accessible and easier to implement. Further, with the emergence of low-cost and service based automated KYC solutions with AI/ML capabilities, pKYC can be adopted irrespective of operation size.

There are many approaches to pKYC adoption. Some FIs adopt a trigger-based approach while others use risk categorisation to make decisions. FIs must have a consolidated view of their customer and business risks, technical capability, data structures, capacity and regulatory compliance pressures across their portfolio, before defining a clear roadmap to pKYC adoption.

Scott Werner an Associate Partner at McKinsey & Company, notes that *"At the core of pKYC is about knowing the 'behaviour' of the customer at any given point in time. What really matters is a 'living' client profile. It is more about good analytics and data rather than technology. There is a case to explore usage of metadata (such as mobile numbers) currently used as part of fraud controls, for AML / pKYC too"*.

KYC-Tech and the importance of Middleware – A PSP FinTech perspective

Many a talented technologist falls for the most obnoxious yet ubiquitous soundbite in the universe of compliance-tech sales pitches, *"This solution / software / tool is fully compliant". The scenario typically involves a vendor that offers some sort of software solution that promises to make firms "compliant"* with some new very complex regulation and is a common occurrence with vendors offering anything from liveness checks to Account Information services.

Good regulation tends to be technology neutral and very rarely a tech solution can be mapped directly to a regulatory provision. When it comes to CDD / KYC, for example, the notion that one vendor / solution is going to address all CDD needs would be facetious. The nature of CDD is precisely to dive deep into the available information and seek more (if necessary) in order to know your customer.

When considering software solutions and in general for compliance-tech, the right approach is perhaps to start from a good understanding of the firms processes and then formulating improvement goals. In payments and in general in fintech, there is a first and foremost obsession with customer experiences, so a key goal may be to build a more customer-centric CDD process where customers are spared from unnecessary paperwork and friction, time-to- onboard is shortened and automation is used whenever possible.

It is also possible that the goal is to simplify a process that is heavily reliant on human-mediated and error-prone subcomponents and / or to improve the compliance posture by making an existing process more robust from the perspective of a new regulatory guideline.

Whilst the steer from senior management will be to "automate more" or to "try to use AI", A good understanding of your compliance operating procedures and a clear mental model of the desired end-state are vital to avoid falling for the "fully compliant" sales pitches.

A thorough review would typically reveal that most KYC / CDD SOPs are relatively complex sets of operations that involve anything from collecting information (sometimes in the form of paperwork issued by competent authorities), verifying it by using reliable sources, setting a risk rating for the customer in question, amongst others. **Javier Pimentel**, Head of Compliance MEA at Amazon note that *"There is no single vendor that can fix all your problems or get you closer to all your CDD process improvement goals in any jurisdiction. I would be really happy to be proven wrong, but my experience is that you will find better answers by looking at Middleware. In fact, and here is my first bold submission, I believe that the best AML-tech (the best compliance-tech in general) is in reality technology that is designed to be very good middleware, i.e. the type of software that different applications use to communicate with each other and is able to act as a bridge for different tools and vendors to be seamlessly integrated into a comprehensive AML / CDD software suite"*.

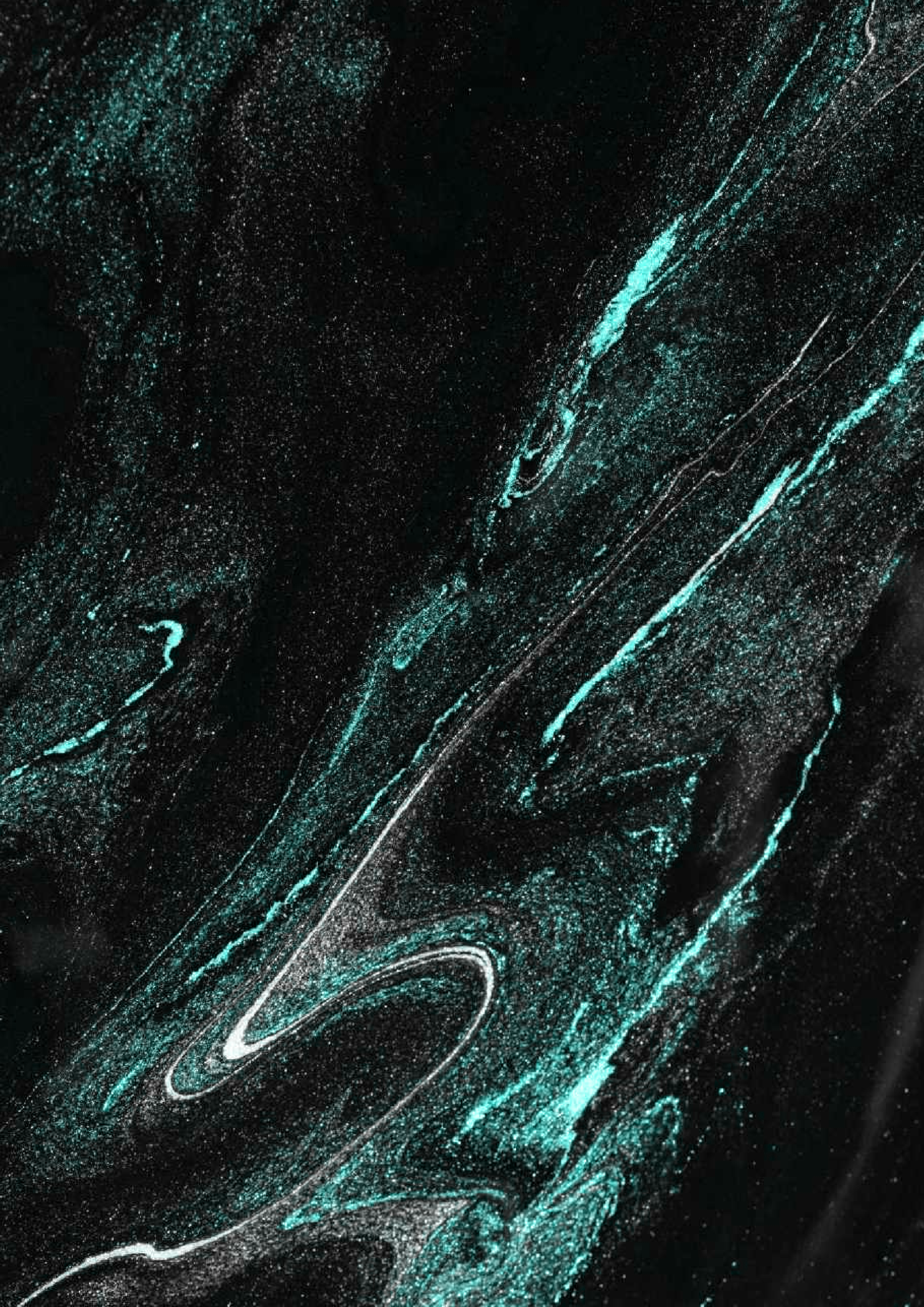
Instead of considering solutions based on features built into the software, consider what integrations are being brought directly out of the box and whether such solutions have or can integrate with the firm's CRM software.

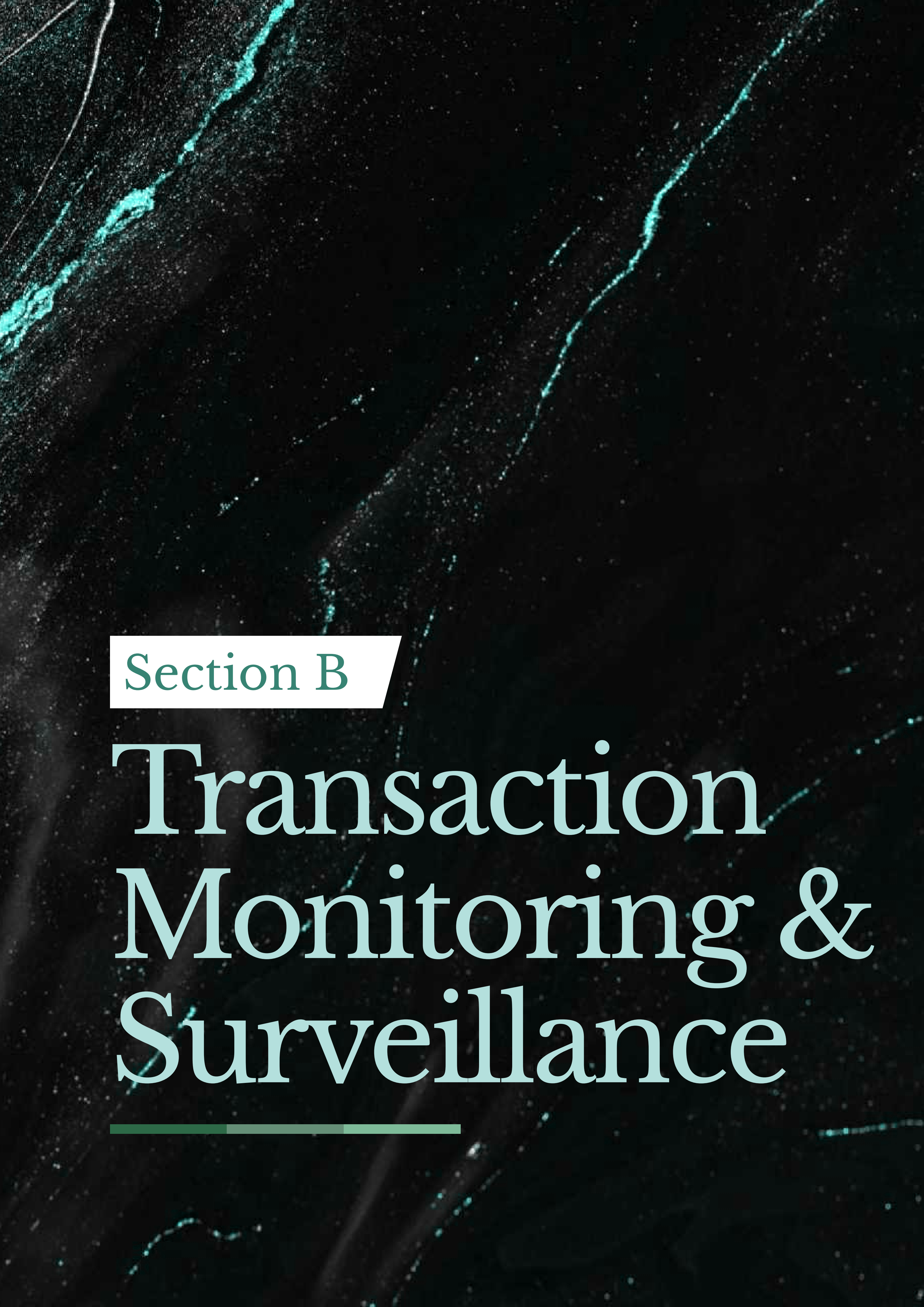
The best CDD processes, especially in a fintech context, are not the ones that overly rely on a feature or a subset of features offered by a single vendor but are instead a mix-and-match of many different tools and technologies from different provenances: AI-based document verification or liveness checks, identity checks based on facial recognition technology, state of the art PEP searches and databases, adverse media web-crawlers.

All of these solutions and tools are so dissimilar that they are never mastered by the same vendor. As a corollary, it is increasingly common that regulators require fintechs / PSPs to implement state-supported ID verification solutions such as the online validation gateway of the Federal Authority for Identity and Citizenship or the UAE-Pass Application, to the point that if you want your CDD process to remain compliant, you have to integrate your compliance tech-stack with these state-supported solutions.

In summary, in the fast moving world of fintechs, no single software or solution is likely to make firms fully compliant out of the box. Solutions that offer flexibility to mix and match and able to stand by a long list of proven and properly functioning integrations with anything ranging from CRM software to state of the art identity verification tools will be successful in that fast paced environment.

> *"Therefore, I submit that at this point in the evolution of compliance tech, the best AML / CDD software suite you can buy is not necessarily the one that the salesmen pitch as the one with the most features to make you "compliant" out of the box, but the one that offers the most flexibility to mix and match and is able to stand by a long list of proven and properly functioning integrations with anything ranging from your preferred CRM software to state of the art identity verification tools"*, summarises **Mr Pimentel**.





Section B

Transaction Monitoring & Surveillance

Introduction

Transaction monitoring (TM) is a framework of automated systems, rules and investigation capability as a key control for mitigating financial crime on a post-facto basis. When unusual transactions are detected, alerts are generated and reviewed by analysts who investigate for criminal activity.

TM and surveillance are crucial for financial institutions as they help mitigate the risks of financial crimes and safeguard the integrity of the financial system. Additionally, they are required by regulators and law enforcement agencies to ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) laws and regulations.

Challenges

Vast changes in the business landscape, fuelled by the growth of fintechs and emergence of payment service providers, payment aggregators, instant payments etc., often subject to differing regulatory standards, has resulted in fragmented local and global transaction flows, a challenging situation for traditional TM programmes that typically operate on a pre-defined set of rule scenarios that identify outlier transactions or activities based on thresholds. These scenarios do not operate at a Know Your Customer's Customer (KYCC) or external entity level, and systems assume pristine data mapping and data quality. TM has evolved at a different pace from the financial industry, and current design has probably gone past its best days. The challenge in operating at a KYCC level is the identification of customers that offer new payment methods (NPMs). Scenarios with long look-backs and limited behavioural profiling capabilities are increasingly stale and too simplistic to flag sophisticated money laundering activities.

Haibo Zhang, a fintech and regtech consultant with extensive experience working at, and supporting, global, US and European financial institutions, agrees. *"Traditional TM will not work in the new landscape. Understanding of typologies, red flags and other criteria needs to undergo a complete change. Previously, technology changed at a gradual pace, but the speed of current change is immense. A complete rethink is necessary, and while action by global agencies such as the OECD and the G20 will help, it will be better if private organisations come together to set standards. Regulators have to keep up, but it is a steep curve."*

Mr Werner, agrees that a change of focus is needed. *"We should be looking for risk signals, not necessarily bad actors. The key is to look for what is normal behaviour so that we can disqualify low-risk data and then look for risk in the rest."*

There is a lot of work to do, but there has to be a paradigm shift. Payment channels are increasing in volume and variety, so it is essential to have a holistic view of risk.

Adoption of automation and machine learning capabilities

Experts' responses to the question on TM suggest that there has been limited success in the use of ML capabilities or automation overall, when attempts were made to replace existing rules-based TM capabilities completely with a Machine Learning (ML) model.

However, there have been some success stories in the use of ML for certain TM processes, for example, segmentation of population for threshold tuning and Robotic Process Automation for data scrubbing and prompting narratives for alert disposition. Scoring and optimisation models are good candidates for automation and machine learning capabilities.

ML models can effectively reduce false positives or hibernate alerts, adding value, reducing processes and costs, and through sharper risk identification, reduce true negatives.

Mr Zhang explains, *"ML can be helpful with segmentation, anomaly detection, facial recognition and possibly NLP. NLP can cover all the 'knowledge bases' for performing coverage assessment, like regulator red flags and internal red flags. Further, If regulators were to consider adding pictures to lists, false positives can be significantly reduced by adding facial recognition to screening inputs."*

Implementation of Holistic / Dynamic Risk Assessment (DRA) model

The traditional risk rating model determines a risk category for each customer using a set of static risk factors during onboarding and again at each periodic review. This model does not consider account activity and behavioural factors and may lack key insights that provide a more accurate understanding of risk.

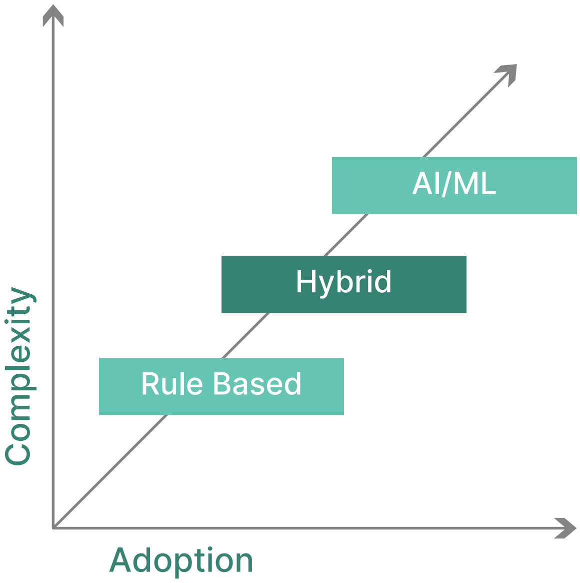
A Holistic / Dynamic Risk Score solves this issue. The risk score combines various risk drivers and behaviours. Behaviours are analysis of the transaction patterns to determine a "degree-of-riskiness". A combined static and dynamic grade provide a final risk score. Used together, DRA and pKYC can potentially provide a higher quality of risk identification and treatment. DRA allows access to data with greater depth and richness, updated dynamically to reflect the most recent insights into the investigation. As a result, financial crime risk can be identified faster with fewer unproductive alerts. DRA also helps create a more robust and accurate assessment of the risk associated with customers.

Paula Borges, former Head of Dynamic Risk Assessment Analytics at HSBC and currently Global Head of Financial Crime Controls at Stripe, noted that, *"Issues are less about the model and more about the data. The chances of success are elevated when institutions focus on getting the basics right i.e. comprehensive and well curated data sets, clear objectives and success criteria, and cover third-party risks, for example, vendor inputs, data, and documentation. It is also critical to ensure robust regulatory engagement right from the beginning. Regulators are keen to see how it goes, and will be open to accept structural change if results are encouraging"*.

Master models

We asked experts whether large master models for transaction monitoring have been considered and if so, what challenges exist in building such models.

The responses suggest that while it would be good to have such models, the maturity level is not yet there.



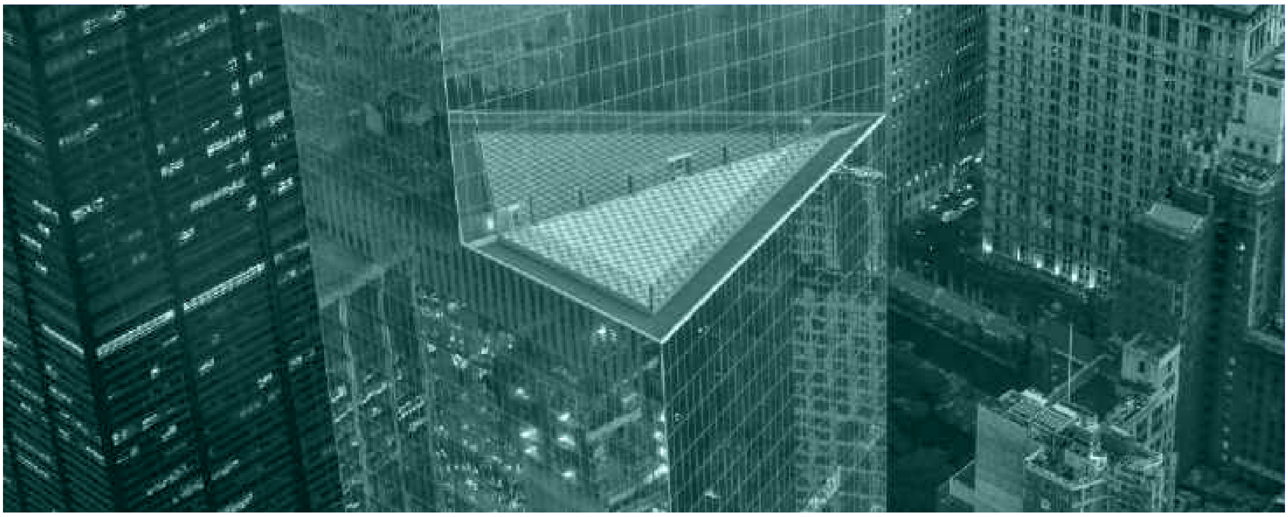
Source: DWG member

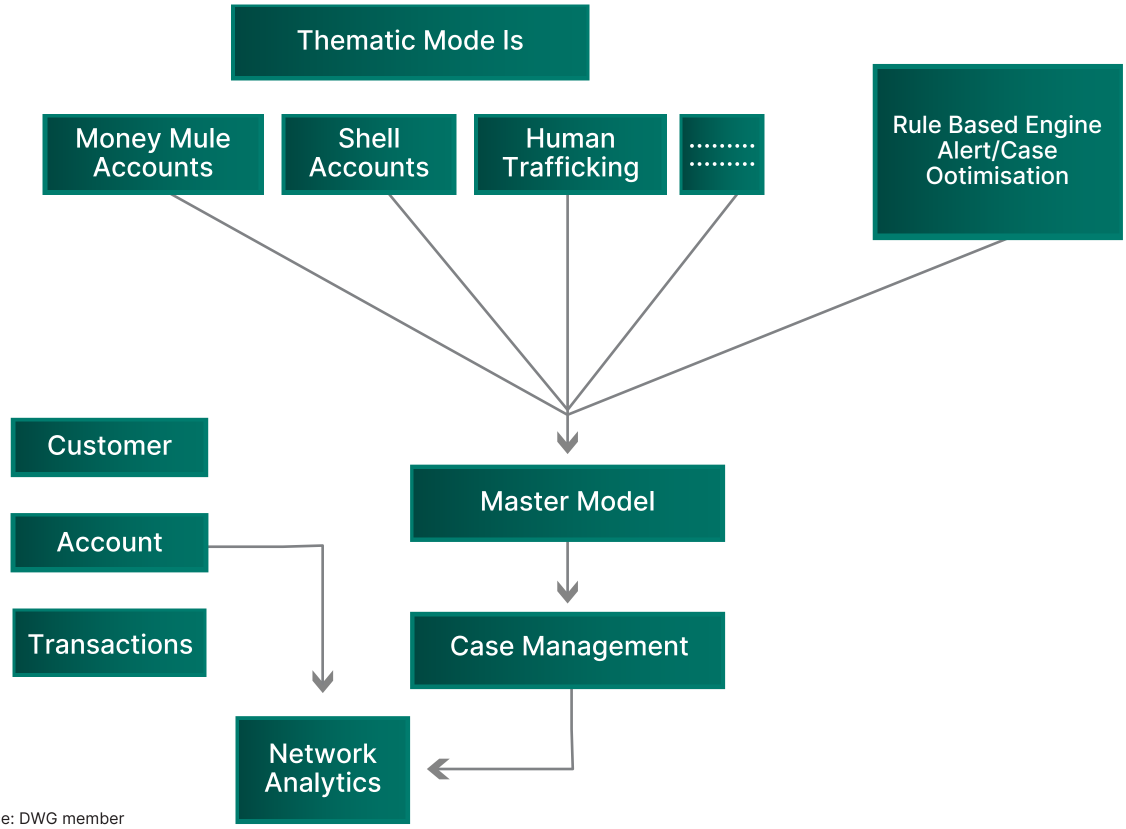
TM models are based on typologies and are preferred by compliance and regulatory teams for their simplicity and explainability, which limits the usage of all-encompassing ML models.

Some experts point out that master models are sometimes limited in their usefulness. *"No-one has successfully created a master model yet, there is no rule set, limited data and explainability is an issue"*, notes **Jas Randhawa**, Founder and Managing Partner of StrategyBRIX, a boutique risk and compliance management consulting business. **Richard Hills** also pointed to limited data as an issue but suggested that *"federated ML may be able to reduce the limitation"*.

Mr Zhang said that master models would need large amounts of data to work. *"It may work for large global banks with internal data flow, but it won't work for smaller banks." "Very few institutions have implemented 100% machine learning models"*, said **David Choi**, a Partner at Oliver Wyman's Digital and Anti-Financial Crime practice.

The operating model needs to change to bring more data scientists and analysts and shift things. A master model could be a behavioural model with more events, data, local explainability, and manual input from relationship managers and branches. Overall, while the idea of a large master model for TM is appealing, there are still many challenges to overcome before it can become a reality.

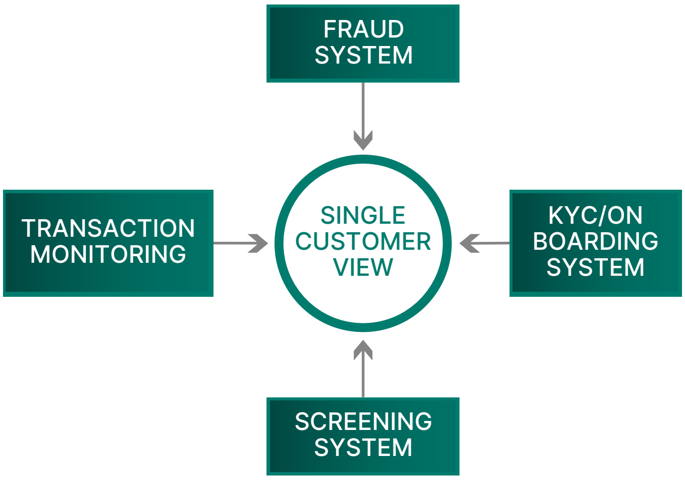




Source: DWG member

Single customer view

There is promise in working towards convergence of various risk identification capabilities across different domains to a single platform. This will reduce overlaps, overheads and provide a holistic view of customer activity and risks. However, it will require organisational changes, changes in the target operating model, organisation culture, leadership, and people. While it may be difficult to have one single investigator to do end-to-end, contextual risk signals can be helpful. Convergence of multiple departments such as TM / Fraud / KYC and dynamic CDD + screening for PEP and adverse media can also be beneficial. A single view of the customer is essential for holistic customer investigation.



Zubin Chichgar, Group Head of Compliance Operations at EmiratesNBD calls out the importance of leveraging the data used by different controls to a common platform, *"Given that the cost of data assembly and mapping is a significant portion of any deployment, and there is a fair degree of commonality of data that's used, the data pool used should be assembled once and then leveraged for multiple purposes. In that, having single platforms being identify various risks would be ideal as it reduces overlaps and overheads as well as gives a wholistic view of customer activity and risks".*

Source: DWG member

Leverage more non-traditional, non-transactional data sets

Relying solely on transactional data for detecting unusual activity will not be sufficient in the future TM domain. Assembling internal and external data, such as KYC data, public domain searches, and company listings, can make the assessment easier and more meaningful. Leveraging rich non-transactional customer data such as biometric and credit card data, can improve risk identification and mitigation.

It is key to understand risk perception and using feeder models to address it. Some institutions are increasingly using non-transactional or asymmetric data sets such as device identity, phone numbers, and email addresses to identify risk and provide additional context to risk events, before they are converted to formal alerts or cases. There is a case to consider closer integration with telcos to obtain additional metadata (of course, within the bounds of customers, age of email addresses, and domain of email addresses) to improve risk identification. Overall, leveraging non-traditional and non-transactional data sets can significantly improve risk identification and mitigation in the TM domain. Assembling internal and external data, using feeder models, and integrating with telcos can help identify and mitigate risks.

Mr Chichgar notes, *"The detection of unusual activity should not be hinging only on transactional data. Any data which can be relied upon should be brought in and assembled to deduce the activity being reviewed. This could be in nature of internal data (transactional data, KYC data, sales data etc) or external data (public domain scrubs for things like tenders, company listings etc). Once the data is assembled, the assessment may prove to be easier and more meaningful"*.

Use of Large Language Models

We asked the experts whether Large Language Models (LLMs) such as ChatGPT can be used to build automated narrative capabilities for case narrative creation, and if so, what are the pitfalls to avoid, especially from a bias/model risk perspective.

Their responses suggest that narrative generators are already used by some institutions, but the systems are slow to mature due to the diverse nature and instances of behaviour and unstructured data. **Mr Hills** warns that narrative generators are still in development. "They can probably be trained using previous investigation outcomes, and probably safe to use for initial work but not to conclude investigations."

The responses also highlight the need to train LLMs with privacy within the firewall and the risks associated with model risk and data privacy. *"Off-the-shelf products will become available, but probably will not be suitable as business models are different across organisations,"* **Mr Randhawa** believes.

Randhawa explains that collaborations with academia institutions have been quite promising. The Proofs of Concept resulted in faster identification of financial crime risk patterns and ML produced better narratives than experienced investigators in a significant number of instances, indicating the potential for disruption. **Mr Randhawa** notes that, *"The risks are also equally high, and mistakes will be amplified due to the systems' scalability. The selective onboarding of risk signals will be much more dynamic, and the machine can ask and extract more specific information to intelligently risk rate customers"*.

In conclusion, while LLMs can be leveraged to build automated narrative capabilities for case narrative creation, there are several pitfalls to avoid, including model risk and data privacy.

Organisations need to train their models internally and selectively onboard risk signals to avoid the amplification of mistakes. The use of LLMs for case narrative creation will be highly disruptive, but off-the-shelf solutions may not work immediately due to the different business models across organisations.

The evolution of technology

The use of ML and AI in transaction surveillance and AML has been a topic of hot debate among experts for a while now. However, there is a significant lack of training data to inform the models on what constitutes unusual activity. Institutions may switch to ML / AI detection systems for efficiency but may not include continuous testing and model maintenance, potentially resulting in misses and regulatory criticism. Therefore, experts emphasise the importance of data hygiene, model development and maintenance rigour, and parallel testing.

To improve the process, external data providers can enrich data, use open source data and intelligence, and facial recognition. Further improvements in models can be applied. Federated machine learning can also have a major impact, as it can overcome data privacy issues. Experts predict that there will be a push to adopt more efficient detection techniques for TM and regulators may focus on getting appropriate coverage over new products and channels such as NPMs and digital assets.

Rules will become a base for the development of optimisation models, ML models, auto RFI, auto closures, and more holistic investigations. However, governance and trustworthy data are issues, and there is a need for standards set for development and usage of ML models. Scoring of alerts and ad-hoc models such as Mule Account detection, Shell Account detection, and thematic models are good use-cases for ML models.

While the use of ML and AI for TM is promising, there is a need for continuous testing and model maintenance, as well as external data providers to enrich data. Federated machine learning can overcome data privacy issues, and there will be a push to adopt more efficient detection techniques for TM.

Use cases

Entity resolution

Entity resolution is a data management and analytics process to identify and link different records that refer to the same real-world entity. This is necessary when dealing with large datasets that contain duplicate or inconsistent records. There are several approaches to entity resolution, including deterministic and probabilistic methods. Deterministic methods rely on the exact matching of attributes such as names, addresses, and social security numbers, while probabilistic methods use statistical algorithms to estimate the likelihood that two records refer to the same entity.

The probabilistic record linkage approach estimates the probability that two records refer to the same entity based on the similarity of their attributes. Clustering algorithms group records that are likely to refer to the same entity based on the similarity of their attributes. Bayesian networks are graphical models that represent the probabilistic relationships between variables and can be used in entity resolution to model the dependencies between different attributes and estimate the probability of a match. Rule-based methods use a set of predefined rules to match records based on specific criteria such as name similarity or address proximity.

Ensemble methods combine multiple algorithms or models to improve the accuracy of the matching process. For example, an ensemble of probabilistic record linkage and machine learning algorithms can be used to achieve better results than either approach alone.

Behavioural Customer segmentation

Customer segmentation divides a customer base into smaller groups based on shared characteristics such as demographics, behaviour, or transaction history. In TM, customer segmentation can provide several benefits, including targeted monitoring, improved detection accuracy, and customised interventions. The methodology for customer segmentation includes behavioural, geographic, risk-based, clustering algorithms, neural networks, and hybrid segmentation. Behavioural segmentation divides customers based on their transaction behaviour, while geographic segmentation divides customers based on geographic location.

Risk-based segmentation divides customers based on their risk profile, and clustering algorithms group customers based on similarity in their transaction behaviour. Neural networks learn from customer data to predict future behaviour. Hybrid segmentation combines two or more methods to create a more comprehensive segmentation approach. The choice of methodology for customer segmentation in TM will depend on the specific goals and objectives of the financial institution, including the availability of data, the complexity of the monitoring system, and the level of risk associated with different customer groups.

Dynamic customer risk scoring (similar to Holistic Monitoring / DRA)

Dynamic customer risk scoring assign risk scores to customers based on their transaction behaviour and other relevant factors in real-time. This process involves analysing customer data, including transaction history, account activity, geographic location, and other demographic and behavioural factors. Machine learning algorithms and other statistical techniques are used to analyse this data and assign a risk score to each customer. The score is updated in real-time as new transaction data becomes available, allowing financial institutions to identify and respond to potential risks quickly.

Experience from a leading Bank in Middle East building a Holistic Scoring Model

Identifying and assessing money laundering risk is a tedious process, as is gripped in a grid of legacy factors such as regulatory requirements and sensitivity of the matter. This makes compliance screening intricate, and consequently leads to an increase in compliance related exits. To deal with such complexity, the Bank has embraced statistical methods that are more dynamic in nature.

For this purpose, sophisticated techniques such as a multivariate scorecard was developed leveraging both Central Bank AML regulatory guidelines and industry best practices. Following robust data science rigor, nearly 550+ variables (features) pertaining to behavioral characteristics of each customer such as transactions in high-risk countries, cash deposits, transaction alerts from different systems anddemographics were its used in developing the final scorecard. Resultant scorecard was then tested for predictive strength and stability and proved to have a superior predictive power while also being stable across time.

It was observed that the proposed classification reduced review base by ~30% while capturing nearly double the number of bad actors.

Benefits of using a holistic scorecard approach:

- Reduced time for implementation and increased accuracy as base extraction is automated and takes majority of the data feed from EDW (data warehouse)
- Comprehensive overview of the customers by using a combination of varied information
- Increasing in efficiency by focusing the resources in the right place and pacing out the review process across quarters so as to achieve timeliness

The methodology used for dynamic customer risk scoring includes supervised and unsupervised machine learning, rule-based scoring, and a hybrid approach. Regardless of the method used, developing a dynamic customer risk scoring model requires access to high-quality data, a deep understanding of customer behaviour, and the ability to analyse large volumes of data in real time. It is also important to regularly test and refine the model to ensure it accurately identifies and responds to potential risks.

Event risk scoring

Event risk scoring is a crucial tool for financial institutions to prioritise investigations and allocate resources based on the level of risk associated with each Event that graduates to an Alert upon breaching a pre-defined threshold. This involves assigning a numerical score to each alert based on predetermined risk factors such as transaction history, geographic location, and transaction amount (and other factors, based on data availability and impact). Risk score is then used to determine the priority of the alert for further investigation or action.

There are three methodologies for alert risk scoring: rule-based scoring, machine learning, and a hybrid approach. Rule-based scoring involves predefined rules to assign a risk score to each alert based on its characteristics. Machine learning involves training a model on a labelled dataset to predict the likelihood of an alert being high or low risk. The hybrid approach combines the strengths of rule-based scoring and machine learning to develop a more accurate and dynamic alert risk scoring model.

The choice of methodology depends on specific requirements of needs the and financial institution and the types of alerts generated by monitoring the system. institutions can transaction Financial reduce their exposure to financial crime and regulatory risk by identifying high risk alerts and investigating them in a timely manner.

Thematic analysis

Thematic analysis can be applied in various ways, such as analysing suspicious transaction reports (STRs), illicit financial flows, and financial crime investigations. By analysing these reports, patterns and trends can be identified, and insights gained into the typologies and methods criminals use to launder money or engage in other financial crimes. Thematic analysis can also be used to analyse the flow of illicit funds through the financial system by analysing data from multiple sources such as transaction reports, public records, and social media. Additionally, it can be used to analyse the results of financial crime investigations, such as Narcotics Typologies, Money Mule Accounts, Shell Company Accounts, Human Trafficking, and Wildlife Trafficking. By analysing data such as case files, interviews, and evidence, themes can be identified that may provide insights into the typologies and methods used by criminals. Overall, thematic analysis can be a valuable tool in fighting financial crime by helping to identify patterns and trends in large volumes of qualitative data and providing insights into typical criminal methods and typologies.

Network analysis

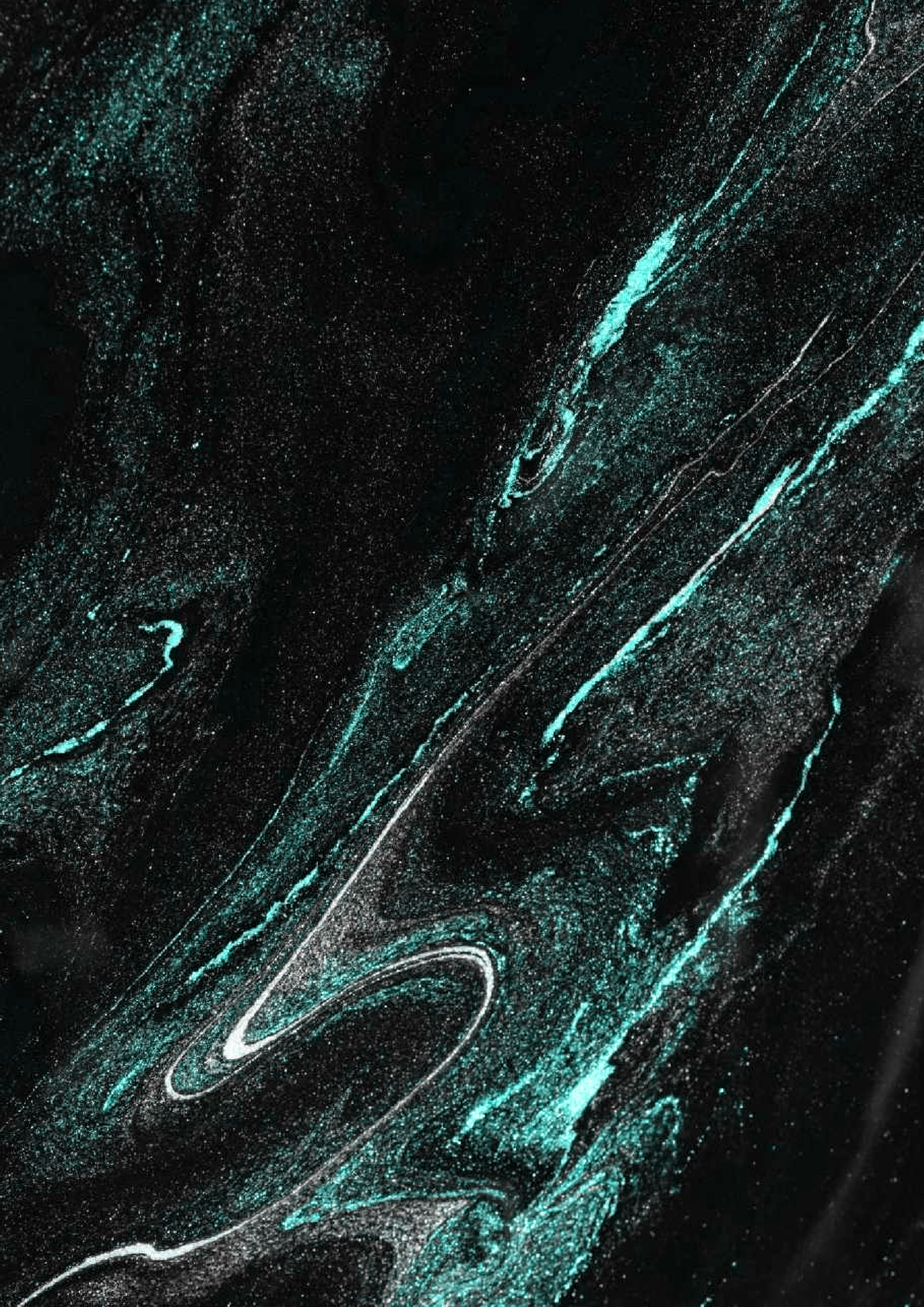
Network analysis tools are used to identify links between different entities and transactions to fight financial crime supporting investigators understand the structure of criminal networks and identify additional suspicious activity. Several types of network analysis can be used, including Social Network Analysis (SNA), Link Analysis, and Flow Analysis. SNA is used to analyse the relationships between individuals or groups, while Link Analysis is used to analyse the connections between different entities such as people, organisations, and accounts. Flow Analysis is used to analyse the movement of money or other assets between different entities. Network analysis is a powerful tool for identifying relationships.

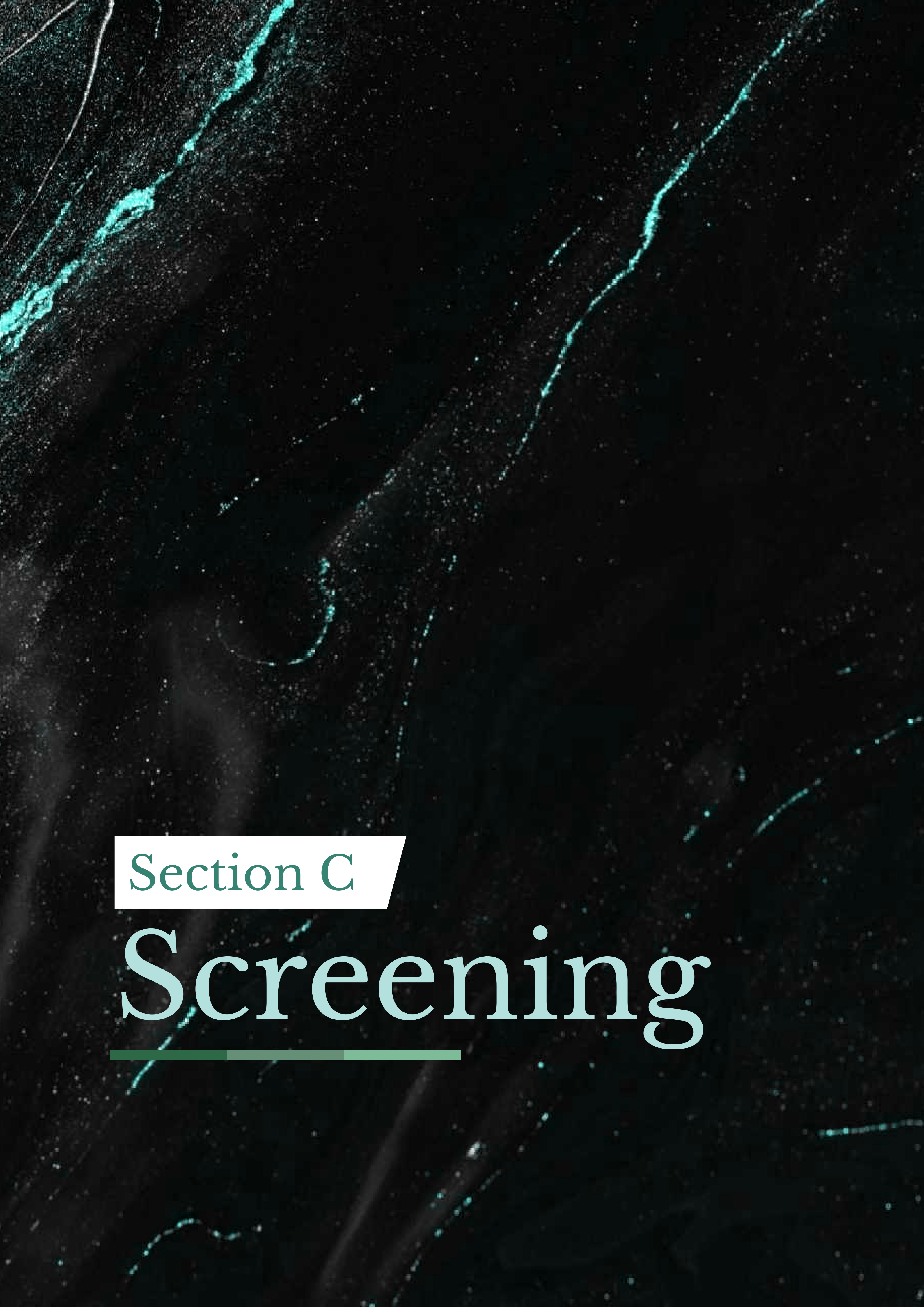
However, it is important to ensure that the analysis is conducted in a way that complies with regulatory requirements and that associated risks are appropriately managed.

Natural language processing

Natural language processing (NLP) uses techniques to extract relevant information from unstructured data sources such as news articles, social media, or case investigation reports. NLP has several applications in AFC, including fraud detection, compliance monitoring and due diligence.

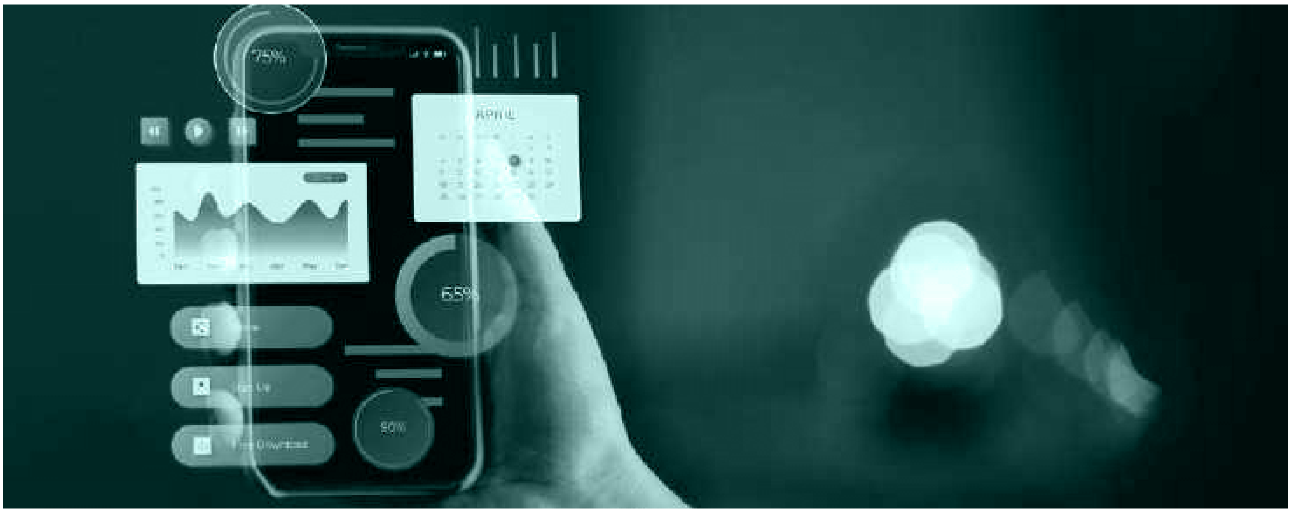
By analysing text data, such as emails, chat logs, and social media posts, NLP can identify patterns of behaviour that may indicate of fraud or other criminal activity. It can also monitor communications between employees and customers to ensure regulatory compliance and analyse public records to conduct due diligence on potential customers, partners, or vendors. NLP allows investigators to analyse large volumes of unstructured data and identify relationships.





Section C

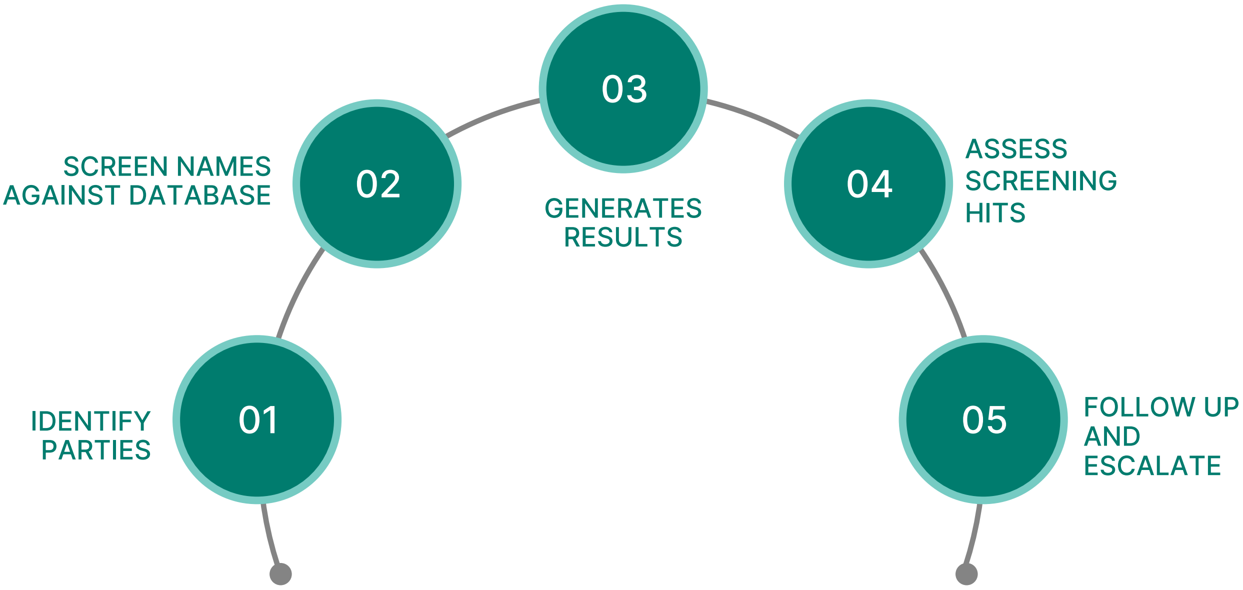
Screening



Introduction

Screening is a fundamental control in mitigating financial crime risks. Typically the screening process consists of customer screening and transactions screening. Customer screening is a process by which financial institutions match names of customers and related parties, such as beneficial owners, authorised signatories, controlling parties etc. against lists designed to identify heightened sanctions, money laundering and reputational risk, such as sanctions lists, Politically Exposed Persons (PEPs) and adverse media lists.

Transaction screening matches names and key criteria against primarily sanctions lists.



Transaction screening involves systematically examining financial transactions to identify and flag potentially matches against lists (sanctions or internal lists). This process typically uses advanced software systems that apply predefined rules, algorithms or machine learning techniques to analyse transactional data. Screening can occur in real-time as transactions are processed or in batch mode, where historical data is reviewed periodically.

Legal and Regulatory Framework

Financial institutions are required to establish comprehensive AFC programmes that include name and transaction screening processes. Non-compliance with these obligations can result in significant penalties, including fines, loss of licenses or criminal prosecution.

Generally, regulators do not have an opinion on the specific technology used, but they believe the use of technology should not transfer responsibility from humans to machines; accountability for outcome remains with the institution. However, there is a recognition from regulators that emerging technologies can enhance and strengthen screening programmes.

Emerging Technologies

As the regulatory landscape continuously changes, a proactive approach is essential to keep up and comply with regulatory expectations and to improve the efficiency and effectiveness of screening. Several regulators have encouraged FIs to leverage technologies like machine learning and robotic process automation (RPA) to transform the screening processes and better manage risk, particularly in the reduction of false positives.

Machine learning is increasingly in use at various elements of screening framework, helping reduce false positives significantly. A number of organisations have replaced first level human review of screening hits with purpose-built ML algorithms for screening name and transactions (payments) and discount these in real time.

However, certain organisations still have a second human analyst (4 eye review) conducted to ensure the algorithm has decided accurately. Institutions with considerable experience in deploying ML algorithms have moved to making 2nd level human review focussed on highest risk cases only, based on their risk appetite and scores.

Challenges

However, algorithm based screening is not without its challenges.

Data quality and bias

ML models rely fully on quality data. If the training data set is incomplete, biased or contains errors, results will be inaccurate or biased, impacting the effectiveness of screening process

Interpretability and explainability

Complex ML models can be difficult to interpret and explain. The lack of transparency can make it challenging to understand how decisions are made, which may raise concerns regarding auditability and accountability. However, this risk can be mitigated to a large extent through careful selection of models (e.g. Decision Tree), focussing on feature importance, usage of various AI explainability tools and robust model performance monitoring and continued testing

Human oversight and expertise

While ML can enhance the screening process, human oversight and expertise remain essential. Human analysts play a critical role in validating alerts, conducting complex investigations and making subjective judgments that require local knowledge and contextual understanding. This is critically important in the light of sanctions circumvention strategies deployed by criminal actors becoming more sophisticated and layered.

A Head of Financial Crime System at Compliance Unit at a UAE Bank points out that the use of machine learning and automation can have significant benefits, but they should first fix data. *"Banks need strong foundations, like proper KYC and good quality data, in place before any of these things should be looked at."*

Dr. Samoj Panicker, Head, Compliance Surveillance Data and Analytics at Standard Chartered Bank notes that bias may not be a major issue in case of standard fincrime processes, *"Explainability is key for the ML models used in TM and Screening. Bias is not such a major one as all the cases/alerts are investigated by many layers of analysts and FCC professionals before a decision is taken. Hence the chance of systemic bias doesn't exist and won't be a factor contributing to the final decision".*

Robotic process automation

RPA technology automates repetitive and rule-based tasks in transaction and name screening, reducing manual effort and increasing efficiency. RPA involves the use of software robots or "bots" to automate tasks traditionally performed by humans, including data extraction and comparison against watchlists. RPA supports:

- Scalability and flexibility
- Error reduction
- Resource optimisation
- Improving audit trail and compliance

Whilst RPA has been somewhat successful in specific areas of processes, it has significant limitations including:

- Complexity of implementation and cost
- Need for verification i.e. ensure bots are programmed accurately, regularly updated to reflect regulatory changes and monitored for potential errors or malfunctions
- Limited to none cognitive abilities

Mr Randhawa expressed concern about RBA. *"The challenge is that no-one is sharing the algorithm logic, but should someone develop an open source LLM model, then RBA might take off".*

Mr Choi notes that *"RPA seems to be lower priority nowadays as many banks have already done this for simpler tasks like investigations data aggregation. Newer technology like LLMs offer potentially more sophisticated automation but comes with more risk".*

Centralized Screening Utility

Insufficient or improper screening can result in a failure to properly scrutinise heightened risk customers or lead to the completion of transactions that are deemed illicit. FIs have spent considerable resources on technology and processes to ensure robust screening to reduce risk.

However, given that a large volume of screening relies on fuzzy matching, the process is inherently inefficient and cumbersome. A majority of alerts are false positives and require significant resources to remediate. Existing cross border payment screening capabilities follow a standard approach of each FI operating their own screening systems and models. A typical cross border payment is screened repeatedly by four or five FIs that facilitate the movement of funds including correspondent banks. This model results in differentiated screening standards and significant customer friction given the need to raise RFIs by Fis to the sending FI and possibly all the way down to the originating FI.

There are several other challenges in relation to traditional screening controls:

- Achieving the right balance between effectiveness and efficiency
- FIs with smaller volumes to screen may struggle to justify the significant investment in a screening solution
- Continual change to risk data and complex requirements create operational challenges
- There is a dearth of skills across the industry and a need for people who understand requirements and can configure the solution
- A single cross border transaction will typically pass through three or more institutions leading to significant duplication in effort.
- Limited information across FIs often results in Request for Information (RFI) to other FIs and, as well as customers, causing time delay and frustration.

To solve this problem, centralised utility-style shared screening capabilities are emerging in the horizon as an alternative offering.

"A well-designed screening programme is an essential control to manage AML and sanctions risks by FIs and to mitigate legal and reputational risks. It is one of the primary controls as part of an overall compliance programme. FIs are obliged to ensure they do not onboard or transact with sanctioned entities, and additionally, it is important to identify customers or associated parties that may represent heightened risk" notes **Praveen Jain**, Head of Client Success at Global Screening Services (GSS) and former MD, Head of Surveillance solutions and Innovation at Standard Chartered Bank.

Centralised solution

A centralisation of the processes across institutions and the building of common utility-based solutions to leverage common platforms, standards and resources will help significantly address many of the current screening challenges.

Benefits of a centralised solution include:

- Reduced costs across institutions by sharing a common infrastructure
- Reduced friction for customers
- Standardised quality of processes and outcomes
- Accessibility to cutting edge technology for all FIs without significant investment
- Easy to leverage the latest technology like cloud-based platforms and the latest solutions available for alert generation, ML – based alert disposition and effective workflow capability
- Reduced complexity
- Improved process for information exchange that will speed up manual alert handling across institutions.

Potential challenges

A centralisation of the processes across institutions and the building of common utility-based solutions to leverage common platforms, standards and resources will help significantly address many of the current screening challenges.

However, a centralised screening solution may not be without its challenges:

- Requirements around data privacy and data localisation in several jurisdictions.
- Adoption of new technology tends to be slow, and many institutions and countries are not comfortable with cloud infrastructure and AI solutions.
- Security and concentration risks from too much reliance on one utility. An issue with infrastructure will impact multiple institutions
- A back-up solution is difficult to build and maintain, especially in the early stages of the utility, which means a lack of a safety net.
- Latency requirements in instant payment and customer onboarding can present a potential challenge in trying to centralise the solution
- The effort involved in building consensus and creating a shared solution

Roadmap

Despite the challenges, there is a definite push towards shared screening infrastructure. Private sector entities have started collaborating FIs to build a transaction screening utility (in PoC form initially), focussed on resolving cross-industry screening challenges by:

- Agreeing common standards
- Sharing information
- Delivering solutions via trusted platforms
- Embracing the best of new technology

Conclusion

Emerging technologies have significant potential in enhancing transaction and name screening as part of AFC programmes, but do not come without challenges.To address the challenges with emerging technologies, corporations must carefully design and implement technology solutions, ensuring proper data governance, ongoing monitoring and model explainability. Collaboration between technologically advanced systems and human experts can leverage both strengths, maximising the effectiveness of AFC programmes.

One of our experts, an experienced compliance executive based in the UAE, stated: *“Firms will always be sceptical about using centralised utility-style shared screening capabilities, but understanding more about the features and functionality, benefits, and integration of these into the existing systems would help aid their decision and, likewise, the future of these capabilities”*.

Marcus Lau, a financial crime compliance professional in Singapore, believes financial institutions prefer an end-to-end solution incorporating identity verification and screening, but there is a lotto consider. *"Employing a third-party centralised screening function would be a trade-off between existing capabilities and efficiencies of a KYC system, incremental operational benefits, and the risk of opening your internal system to an external source."*

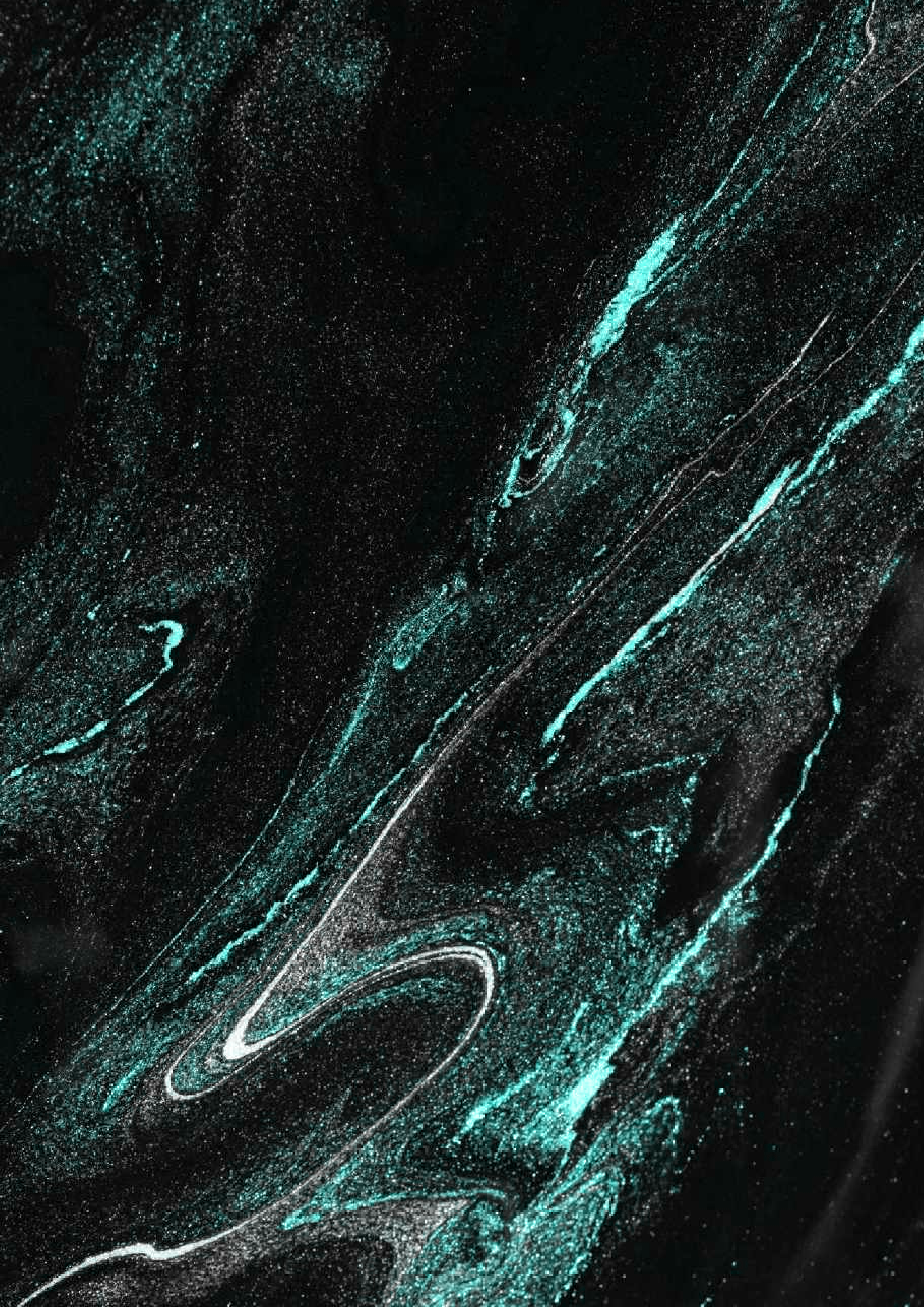
Name screening has been attempted as part of KYC utilities but has not yet been successful at scale. Perhaps a national or regional level name screening solution in the same lines as a shared utility is possible. Further technology innovation, such as privacy enhancing technology, will also make sharing of intelligence in such utilities easier and provide further customer benefits.

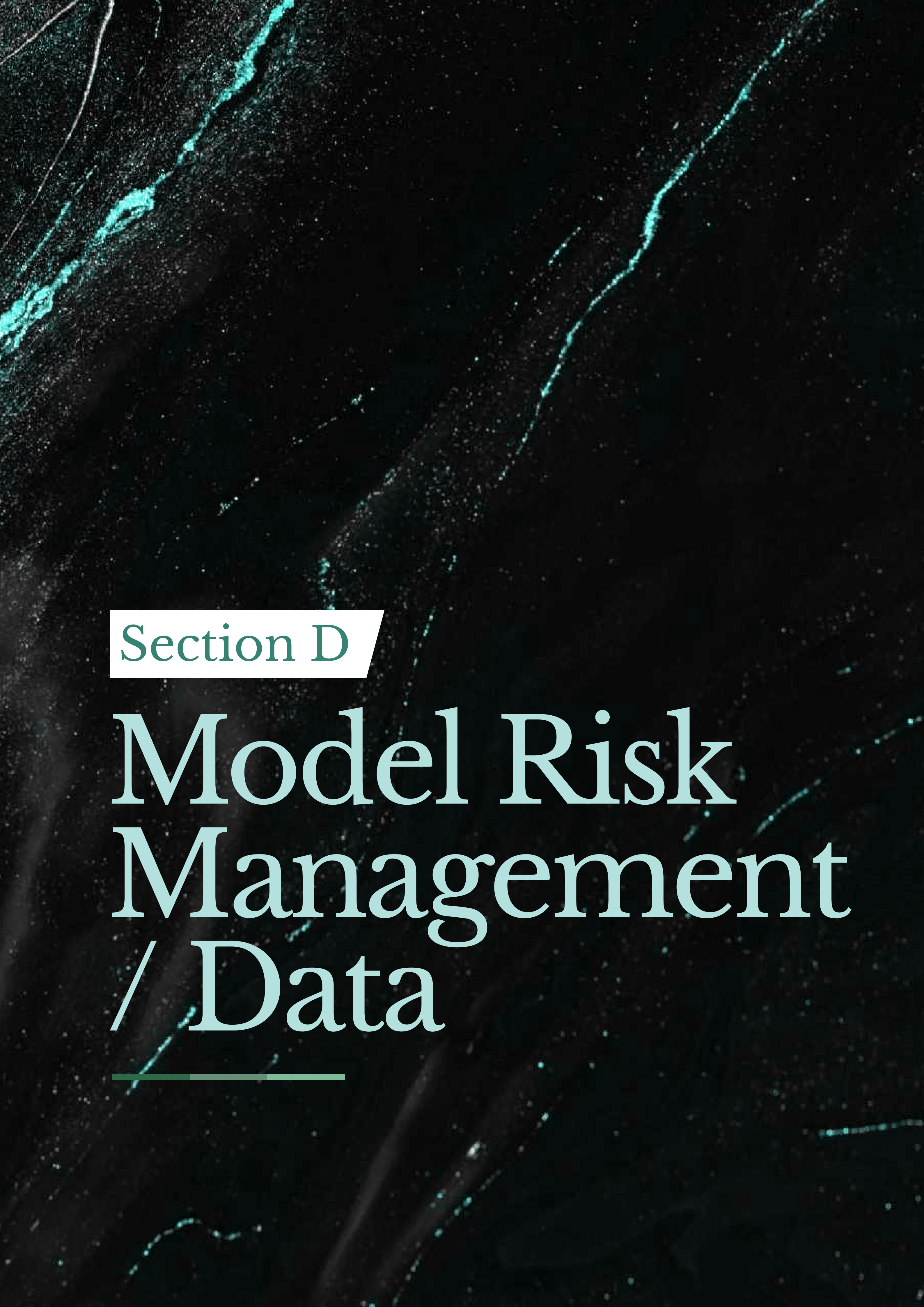
Mr Randhawa believes that adverse media screening will be significantly transformed: *“Adverse media screening is a major pain point for FIs, and PEPs are also expensive to manage. Adverse media is the most possible case for LLM disruption.”*

Mr Choi notes that, *“FIs have relied on external data providers (e.g., sanctions lists, country risk, Id verification) and there are now vendors that extract, categorize and even risk rank public information for tasks like negative news searches. There is no [one single] standard in these data sources though and I would expect that it will continue to be a fragmented market given the various data requirements, and the varied data privacy laws globally that make it challenging to have a single provider(s)”*.

It is also important to note that while these emerging technologies hold significant potential, their adoption in AFC programmes must also consider ethical considerations, data privacy and regulatory compliance. Corporations need to ensure that these technologies are deployed in a responsible and secure manner, with appropriate safeguards to protect sensitive customer information and maintain compliance with relevant laws and regulations.

Some practitioners have emphasised the importance of acknowledging the significant investment required in both time and effort to set up a centralised system and get it working efficiently. The cost and effort will add to a KYC system’s current cost and effort. It is a long-term investment, and the fact that no cost savings are realised immediately until finalised makes it not an easy business case.





Section D

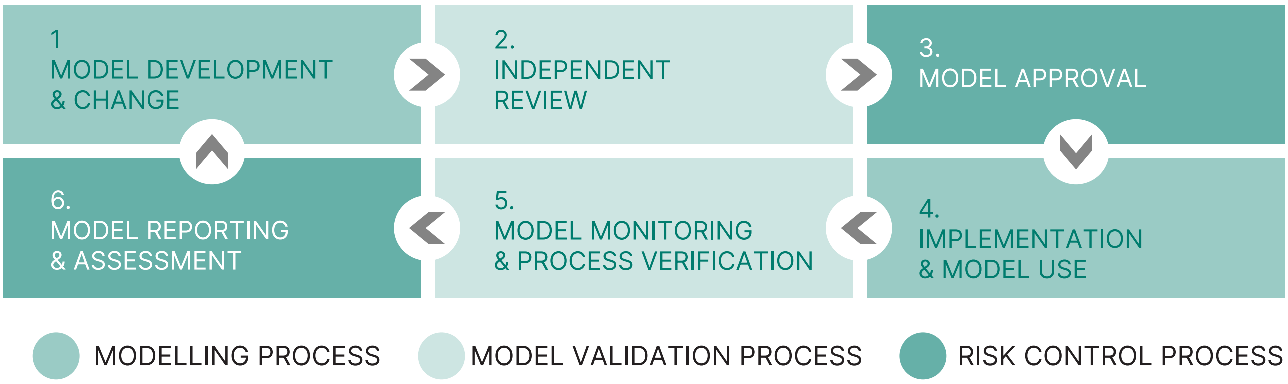
Model Risk Management / Data

Model Risk Management Framework

Financial institutions use financial and economic models to manage capital and risk, and for decision-making. The use of these models, regardless of design and governance, introduces a certain amount of risk. Increasingly, AFC models are being classified as models and thus subject to model risk management rigor.

The Model Risk Management Framework (MRMF) is a set of guidelines and best practices designed to help organisations identify, assess, and manage risks associated with using models in their operations.

DIAGRAM: THE MODEL LIFCYCLE



1 MODEL DEVELOPMENT & CHANGE

2. INDEPENDENT REVIEW

3. MODEL APPROVAL

4. IMPLEMENTATION & MODEL USE

5. MODEL MONITORING & PROCESS VERIFICATION

6. MODEL REPORTING & ASSESSMENT

● MODELLING PROCESS ● MODEL VALIDATION PROCESS ● RISK CONTROL PROCESS

Source : Model risk management principles for banks, supervisory statement | SS1/23, May 2023, Bank of England PRA

A robust MRMF typically includes the following components:

Model inventory and classification

An inventory of all models used within the organisation, classified according to complexity, criticality, and impact on business operations. This step is crucial in identifying the models that require the most attention and resources

Model validation

An assessment of accuracy, reliability, and appropriateness of the models should include testing the models under various scenarios and ensuring they are properly calibrated. This step helps ensure that the models are fit for purpose and produce accurate and reliable results

Model governance

The establishment of policies and procedures for the development, implementation, and maintenance of models to ensure the models are consistent with the organisation's risk appetite, ethical standards, and regulatory requirements. This checks that the models are developed and used in a responsible and ethical manner

Model documentation

Documentation of the development, implementation, and maintenance of models, which includes all assumptions, data sources, and methodology used. This step helps ensure that the models are transparent and that their development and use can be audited and reviewed

Model performance monitoring

The ongoing monitoring of performance to ensure they meet the organisation's needs and expected goals. This step helps ensure that the models produce accurate and reliable results and that any issues are identified and addressed promptly

Model change management

Establishing procedures for managing model changes, including assessing the impact of the changes on performance and the organisation's risk profile. This step helps ensure that any changes to the models are properly assessed and the risks associated with the changes are effectively managed and mitigated Overall, a robust MRMF is essential for managing the risks associated with using models in financial institutions. It helps ensure that models are accurate, reliable, and appropriate for business operations, and that the risks associated with their use are effectively managed and mitigated. By implementing a comprehensive MRMF, financial institutions can improve their risk management practices and enhance their overall performance.

Equally, it is important that AFC professionals spent sufficient time collaborating with he independent model review teams, as often, model reviewers may not fully understand AFC risks, apply protocols relevant for financial risk model evaluation, causing incorrect outcomes.

> **Mr Choi** notes, *"[In relation to] model risk management skills, AFC teams undertaking more advanced or AI-based solutions need to be able to explain and document these solutions to MRM team. The explainability of these solutions will be critical to wider adoption. AFC teams need to take stakeholders like MRM and regulators on the journey to transition to AI-based solutions".*

AI-based solutions need to be able to explain and document these solutions to MRM team. The explainability of these solutions will be critical to wider adoption. AFC teams need to take stakeholders like MRM and regulators on the journey to transition to AI-based solutions.

Model identification

This involves establishing relevant criteria for identifying the model

Model risk assessment

This entails evaluating the magnitude and significance of the identified risks, considering factors such as the complexity and criticality of the models, potential impact on business decisions and regulatory requirements, eventually leading to model nsk classification

Model risk mitigation

This includes implementing controls and measures to reduce the identified risks to an acceptable level. It may involve model validation, robust model development and implementation processes, data quality assurance and model governance frameworks

Model risk monitoring and maintenance

Models need to be continuously monitored and reviewed for their performance over time to detect any emerging risks or deviations from expected behaviour. This includes ongoing model validation, performance monitoring and periodic reassessment of risks

Reporting and governance

This refers to delineating responsibility, accountability, and govemance in MRM. It includes defining roles and responsibilities, documenting policies and procedures, and ensuring effective communication and reporting to stakeholders, including senior management and regulators

Source : MRM in times of AI : Model risk management for banks in the AI paradigm takes off from the traditional craft, June 2023, CRISIL Global Research & Risk Solutions

Use of emerging technologies in MRM

Several emerging technologies can enhance the MRM process, such as AI and ML, natural language processing (NLP), potentially blockchain and cloud computing.

AI and ML can be used to automate the model validation process, improving speed and efficiency. These technologies also improve accuracy by analysing large volumes of data and identifying patterns and trends that humans may miss. NLP can automate the review of model documentation and identify potential errors or inconsistencies. It can also analyse qualitative data such as regulatory reports and customer feedback to identify emerging risks or areas of concern.

Blockchain technology can enhance the transparency and traceability of model development and validation and create secure and auditable records of model usage and changes. Cloud computing, on the other hand, can improve the scalability and flexibility of MRM systems. By leveraging cloud infrastructure, financial institutions can more easily manage large volumes of data and scale their MRM systems as needed.

Finally, RPA can automate repetitive tasks such as data entry and report generation, freeing MRM professionals to focus on higher-value activities such as model validation and risk assessment. Overall, these technologies have the potential to enhance the effectiveness and efficiency of MRM processes, reduce costs, and improve risk management outcomes.

However, it is important to ensure that implementation is compliant with regulatory requirements and that the risks associated with their use are appropriately managed. It is crucial for financial institutions to carefully evaluate the benefits and risks of each technology and develop a comprehensive strategy for their implementation.

Data Quality Management Framework

A Data Quality Management Framework (DQMF) is a comprehensive set of guidelines and best practices that an organisation implements to ensure that its data is accurate, complete, consistent, and timely. The framework comprises several components that work together to achieve this goal.

Data governance involves establishing policies and procedures for managing data within the organisation. This includes defining roles and responsibilities, ensuring compliance with regulatory requirements, and establishing data standards. By doing so, the organisation can ensure that data is managed consistently and effectively across all departments.

Data quality assessment involves assessing data quality across various criteria such as accuracy, completeness, consistency, and timeliness. This includes identifying data quality issues, analysing their impact on business operations, and prioritizing them for resolution thereby enabling identification of areas where data quality needs improvement and take corrective action. Data profiling is the analysis of data to understand its structure, content, and relationships through identification of patterns, trends, and anomalies in the data and assessing their impact on data quality thereby helping organisations gain insight into data quality and take corrective action. Data cleansing corrects or removes data that do not meet quality standards. This includes standardising data, removing duplicates, and correcting errors. Data monitoring is the ongoing scrutiny of data quality to ensure it meet the organisation's standards. This includes identifying and addressing data quality issues as they arise. Data quality reporting provides data quality metrics to stakeholders within the organisation. This includes providing regular reports on data quality performance and identifying areas for improvement.

A robust DQMF ensures that an organisation's data is reliable and trustworthy for informed decision making compliant with regulatory requirements. By implementing the components of the DQMF, organisations can ensure that their data is accurate, complete, consistent, and timely, which is critical for their success.

Responsible AI-Overview

Responsible AI refers to the ethical and socially responsible use of AI technologies. AI technologies have the potential to impact many aspects of society, and any AI system should be designed and implemented in a way that is transparent, fair, accountable, and inclusive.

There are several key principles to ensure that AI systems are developed and used responsibly:

AI systems should be transparent and explainable so that users understand how decisions are made	AI systems should be designed to avoid bias and ensure fair outcomes for all users	AI systems should protect the privacy and security of user data	Organisations that develop and use AI systems should be accountable for their actions and decisions	AI systems should be designed to be robust and reliable and to mitigate the risk of errors or unintended consequences.

Global organisations are developing AI ethics frameworks that typically include principles for responsible AI, and tools and processes for implementation. Examples include the IEEE Global Initiative for Ethical Considerations in AI and Autonomous Systems, the Montreal Declaration for Responsible AI, and the European Union's Ethics Guidelines for Trustworthy AI.

Responsible AI is an important concept that recognises the potential of AI to do both harm and good and seeks to ensure that AI is developed and used in a way that benefits society. It is important to understand these principles and to promote their adoption.

Use of technology – Responsible AI

Several technologies and techniques can be used to help ensure responsible AI systems:

Explainable AI (XAI), designed to make AI systems transparent. XAI explains how decisions are made and helps to identify potential biases and improve the fairness and accountability of AI systems

Synthetic data generation creates artificial datasets to mimic real - world data without using sensitive information.
This allows the testing of AI systems without compromising the privacy or security of real data

Adversarial testing checks for weaknesses by using flawed data, data with a potential bias, for example, to ensure robust systems

Differential privacy ensures that individual user data remains private and secure, even when used to train AI systems.
This is particularly important in preventing the misuse or abuse of user data by AI systems

Human-in-the-loop testing is an emerging technology that involves having human experts review and validate the outputs of AI systems. This can help to ensure that AI systems support appropriate and ethical decision making, and can improve on accuracy and reliability.

Use of emerging technologies in DQMF

Emerging technologies have the potential to revolutionise the way we manage data. AI and ML can automate data cleansing and normalisation processes. By identifying patterns and anomalies in data, AI and ML can also help detect data quality issues that may have gone unnoticed otherwise. Another emerging technology, blockchain, can enhance data quality management frameworks. By creating secure and auditable records of data transactions, blockchain technology can improve the traceability and transparency of quality management processes.

Cloud computing can enhance data quality management frameworks. By storing and managing large volumes of data, cloud computing can improve accessibility and availability. Additionally, it can provide data quality management services on a scalable and cost-effective basis.

These emerging technologies can potentially to enhance the effectiveness and efficiency of data quality management frameworks. By reducing costs and improving data-driven decision-making outcomes, these technologies can help organisations stay competitive in today's data-driven world. However, it is important to ensure that these technologies are implemented in a way that is compliant with regulatory requirements and that the risks associated with their use are appropriately managed.

Challenges

Experts were asked about the impact of applying model risk management standards to end-to-end transaction monitoring and screening. They suggested that while scenarios based on typologies used in TM processes are simple and straightforward and may not qualify as models per se, optimisation and scoring models using machine learning methods may qualify as models from an MRM perspective.

Mr Hills believes there is a lack of understanding of what is needed. *"We need to work with regulators to come up with standards on what ML models are acceptable, advisable, and for what problems. We need to inform and update the knowledge base in this area, we need more forums to talk about these issues and form views"*.

Data challenges, such as the lack of historical data, real-life events, lack of information, and feedback from the Financial Intelligence Unit (FIU) are an inhibiting factor.

The use of traditional MRM techniques on financial crime models that deploy machine learning models presents several challenges. One approach to screening solutions is model testing, while model validation / replication and testing can be considered for scoring/optimisation solutions.

However, the biggest risk is that people may not understand many parts of the nature of financial crime, resulting in evaluating components of the model to outcomes that are unrelated. While many people are qualified in statistics and math, their ability to put it in the context of financial crime realities is limited, sometimes causing more harm than good.

Experts emphasise the importance of explainability in ML models used for TM and screening while downplaying the significance of bias due to multiple layers of investigation by analysts and FCC professionals. However, challenges such as data drift, product changes, and payment platforms can lead to issues with bias, client types, segments, cultural names, affiliation, and controls.

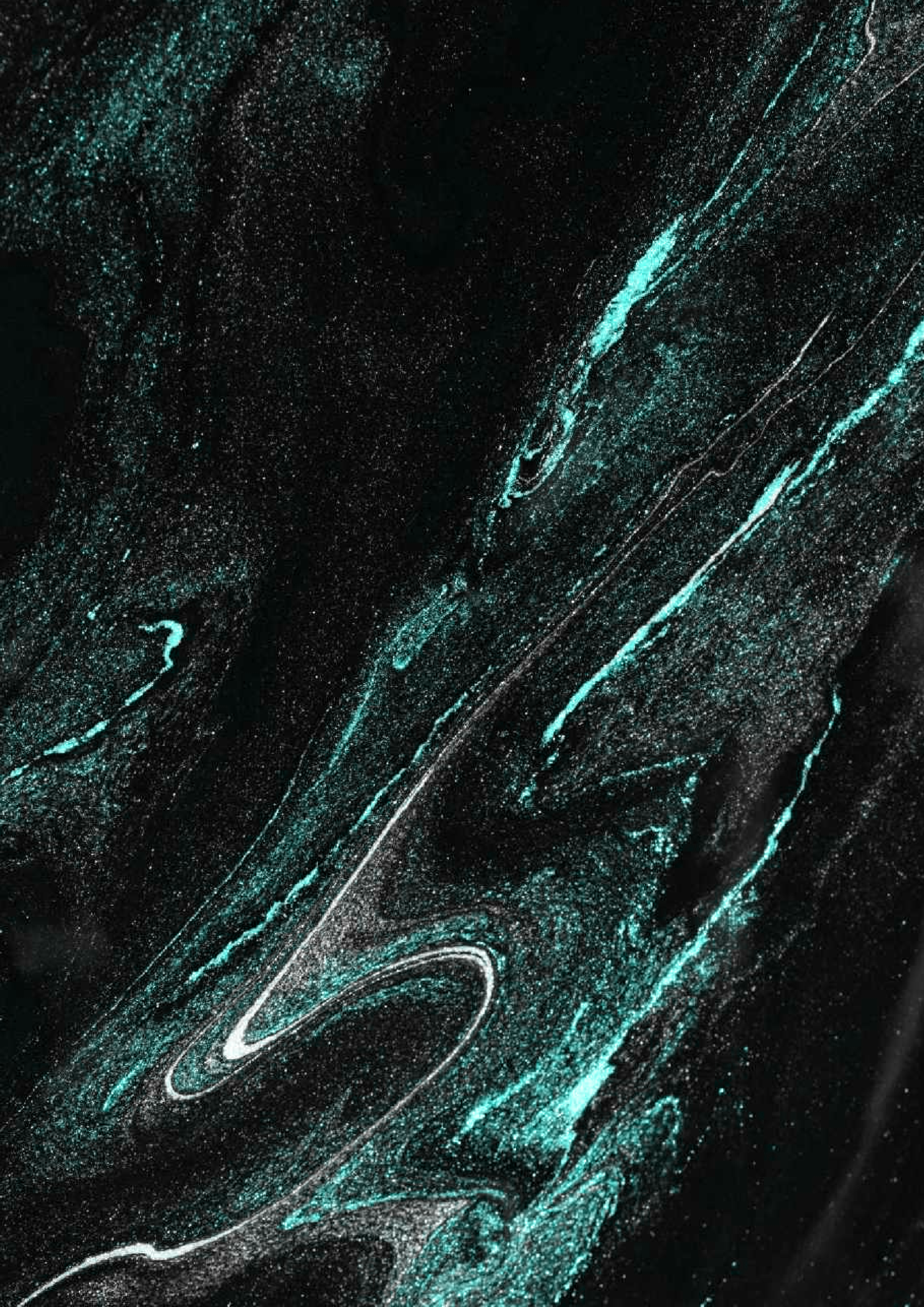
ML models are not being adopted as widely as they could be due to several factors, according to experts. One solution proposed is to group ML models based on their level of risk, as the EU has done, to focus on the most critical models.

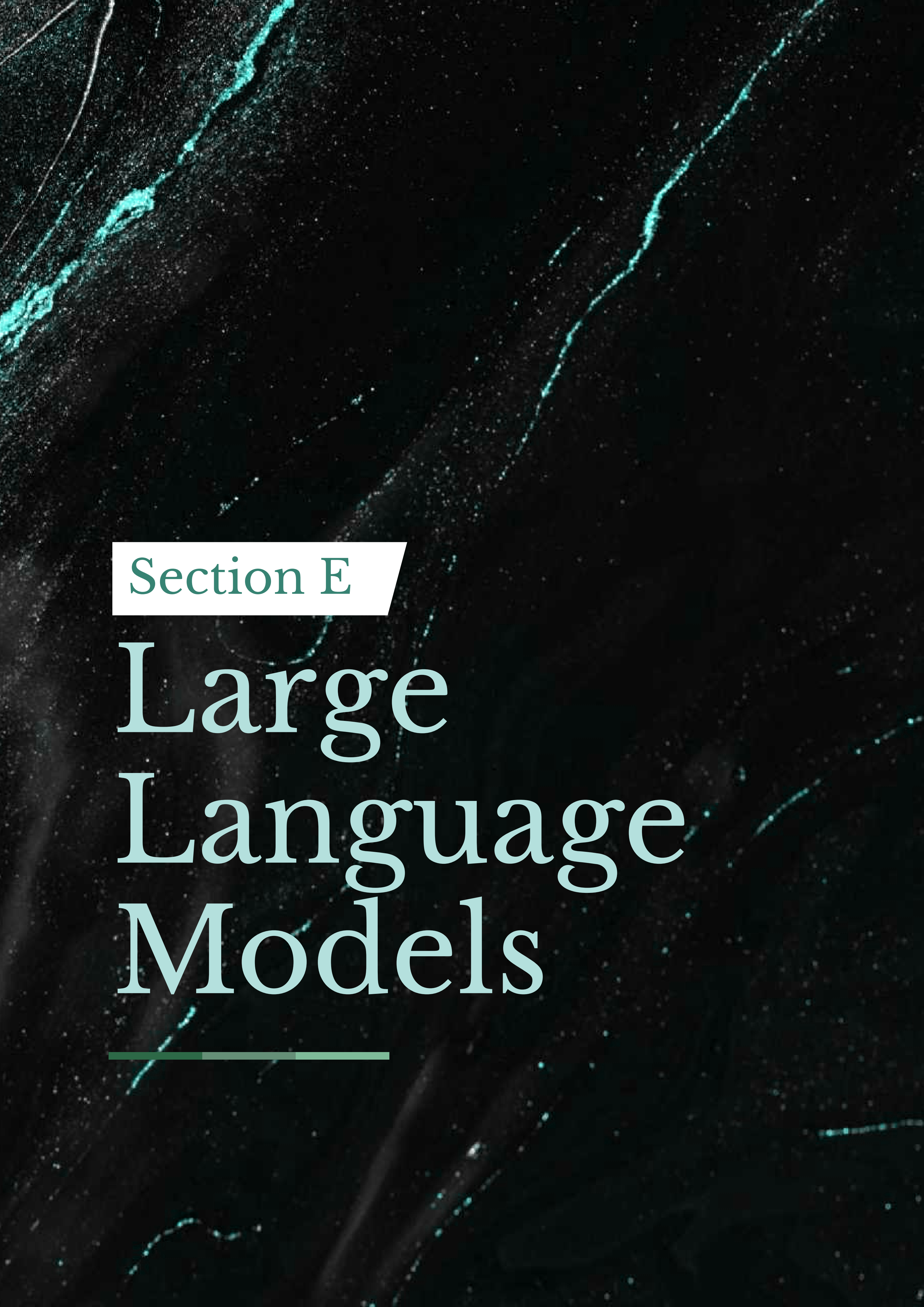
There is a disconnect between the understanding and skill sets of banks and vendors, particularly in rule-based models and MRM, scenario models, fundamental standards, and fuzzy logic / rule models. Another issue is the disconnect between Model Risk Management and Regulatory Financial Risk System, as well as data challenges such as target variable issues and data availability. Technical soundness is solvable, but the challenge is convincing regulators.

Experts suggest that while end-to-end TM and screening may not qualify as models, optimisation and scoring models using ML methods may qualify as models from an MRM perspective. Hills also believes there is a need to work with regulators to develop standards on what ML models are acceptable and advisable for what problems and to have more forums to talk about these issues and form views.

Dr Panicker calls out the importance of building strong governance over AI / ML models *"[Organisations should build] guardrails to ensure transparency in the use of AI. These include registry of all the AI/ML based solutions, identifying the risk of each of the solution through extensive questionnaire, strong and independent second line challenge and explicit endorsement of the solutions by senior stakeholders"*

The experts also highlighted data challenges and the need to understand the role of each component of the model, including judgment, to overcome limitations and issues.





Section E

Large Language Models

Introduction

Large language models (LLMs) have emerged as powerful tools in the domain of natural language processing, offering extensive capabilities in understanding and generating human-like text, in the last 12 months. In the financial services industry, particularly in areas concerning financial crime prevention, Know Your Customer (KYC), and screening processes, LLMs have great potential to play a significant role. This section explores the potential use cases of LLMs in these areas and delves into the characteristics of a robust architecture that can efficiently incorporate these models and also provide a short summary of the steps followed a mid-size FI in the UAE to deliver a PoC on LLM for TM narrative generation.

Potential Use Cases of LLMs in Anti Financial Crime, KYC and Screening

In the ever-evolving financial crime landscape, the emergence of Generative Artificial Intelligence (gen AI) has sparked unprecedented interest.

Gen AI's ability to synthesise vast quantities of data, capacity for advanced and nuanced analysis of complex datasets, and rapid learning pace make it incredibly well suited to addressing challenges in the financial crime space.

> **Charmian Simmons** and **Eve Whittaker** of Sensa-NetReveal notes that *"Integrating gen AI into AML compliance and fraud platforms demands careful consideration . Foundational model design, ethical and operational implications, as well as privacy concerns, model transparency, and regulatory alignment, are often top-of-mind. Maintaining a balance between automation and human expertise is pivotal to avoid blind reliance on technology and inaccurate outcomes"*.

Fraud Detection

LLMs can be utilised to analyse transaction patterns and customer communication to identify anomalies or suspicious behaviour indicative of fraud. By understanding the context and nuances in text data, LLMs can help in detecting phishing emails, fraudulent claims, and other types of scams. For instance, a sudden spike in transaction volume, transactions in high-risk jurisdictions, or transactions with unusual descriptions can trigger alerts for further investigation. Fraudsters often use phishing emails or fraudulent communications to trick individuals or businesses into disclosing sensitive information or making unauthorised transactions. LLMs can potentially be trained to recognise the linguistic patterns and tactics commonly used in such communications, helping to filter out phishing emails and alerting users to potential scams.

KYC

LLMs can assist in verifying the authenticity of documents submitted by customers. By analysing the text and structure of documents, LLMs can identify inconsistencies or alterations that may indicate forgery and can potentially be used to cross-verify information provided by customers against external databases and publicly available information.

Adverse media summary generation

LLMs can scan through vast amounts of news articles, social media posts, and other textual content to identify adverse information related to customers or transactions. Through sentiment analysis, LLMs can help understand context and sentiment of the content they scan, enabling identification of genuinely adverse information and false positives, thereby increasing the accuracy of the screening process.

EDD processes

LLMs can potentially automate parts of the EDD process, gathering and analysing additional information to provide a thorough assessment of money laundering risk. AML regulations are constantly evolving, and financial institutions must stay up to date to ensure compliance. LLMs can be used to track changes in AML regulations and guidelines, ensuring that internal policies and procedures are always in alignment with regulatory requirements.

In summary, LLMs offer a versatile and powerful toolset for enhancing AML efforts within financial institutions. Through advanced analysis of transaction data, customer profiling, regulatory compliance, and continuous learning, LLMs contribute to a more secure and compliant financial ecosystem.

In summary, Large Language Models offer a powerful set of capabilities for enhancing adverse media screening processes in financial institutions.

Important Architecture elements to consider for LLMs

Key considerations whilst developing an architecture for LLM PoCs and deployment:

- **Data ingestion layer**
  Collects and preprocess data from various sources, including transaction data, customer information, external databases, and media sources, requires components like data connectors, preprocessing modules, and data validation tools

- **Storage and data management**
  Stores and manages large volumes of data securely and efficiently, requires components like database systems, data lakes, and data warehousing solutions

- **Large language model layer**
  Performs natural language processing, pattern recognition, and risk assessment, requires components like pre-trained LLMs, fine-tuning modules for domain-specific knowledge, and model management systems

- **Integration layer**
  Integrates the LLMs with existing systems and workflows within the financial institution, requires components like API gateways, middleware, and workflow management tools

- **User interface and reporting**
  Provides users with access to the results, insights, and recommendations generated by the LLMs, requires components like dashboards, reporting tools, and alerting systems

- **Security and compliance**
  Ensures that the architecture adheres to regulatory requirements and protects sensitive customer data, requires components like encryption tools, access control systems, and compliance monitoring solutions

- **Continuous learning and feedback loop**
  Enables the LLMs to learn from past cases, user feedback, and new data to continuously improve performance, requires components like feedback mechanisms, re-training pipelines, and performance monitoring tools.

Pros and cons of an LLM infrastructure / architecture

Whilst these are early days, experts share the following throughs on pros and cons of a LLM based architecture for the future AFC framework.

Advantages may include:

- **Scalability** The architecture is designed to handle large volumes of data and numerous transactions, ensuring that it can scale to meet the needs of the financial institution

- **Accuracy** The use of LLMs enhances the accuracy of risk assessments, fraud detection, and customer profiling

- **Efficiency** Automation of various processes leads to increased efficiency, reducing the time and resources required for KYC, screening, and financial crime prevention

- **Compliance** The architecture includes specific components for ensuring regulatory compliance and data protection, helping financial institutions adhere to legal requirements.

- **Continuous improvement** The inclusion of a feedback loop and continuous learning mechanisms ensures that the system improves over time, adapting to new patterns and risks.

Disadvantages may include:

- **Complexity** The architecture is complex, requiring significant resources and expertise to implement and maintain

- **Dependence on data quality** The effectiveness of LLMs is heavily dependent on the quality of the input data. Poor data quality can lead to inaccurate results

- **Potential for bias** If the LLMs are trained on biased data, they can perpetuate and amplify these biases in their assessments and recommendations

- **Security concerns** The storage and processing of large volumes of sensitive data pose significant security challenges, requiring robust protections to prevent data breaches

- **Cost** Implementing and maintaining this architecture can be costly, requiring investments in hardware, software, and human resources.

> **Mr Choi** highlights challenges that FIs should keep in mind whilst embarking on the LLM journey. *"LLMs are able generate text for use cases like transaction monitoring case narratives but FIs cannot rely on LLMs for without stringent oversight and testing from an AML practitioner. But as FIs learn to incorporate LLMs into their processes with appropriate governance and as vendors expand their platforms to incorporate LLMs targeted for AML, I would expect that the usage of these solutions will grow quickly".*

Implementing a Proof of Concept (PoC) is a critical step in assessing the viability and effectiveness of LLMs in financial crime prevention, KYC, and screening processes. Below are standard steps, a detailed approach, and typical timelines for running a successful PoC.

Standard Steps for a PoC

- Clearly define scope of PoC and establish boundaries
- Engage key stakeholders
- Choose an LLM solution or vendor that aligns with objectives and technical requirements
- Gather and prepare necessary data for PoC
- Set up necessary hardware and software environment for the PoC including provisioning servers, installing software, and configuring network settings
- Train or fine-tune LLM on specific data to ensure it is adapted to the nuances of use case
- Run tests to evaluate performance of LLM in real-world scenarios
- Analyse results and gather feedback
- Document findings

Key elements to consider include:

Resources

Project manager, Data scientists / ML engineers, Data engineers, Software developers, Risk and Compliance Officers, Domain experts, IT support, End-users / analysts

Technology

Machine learning frameworks (Such as TensorFlow or PyTorch for developing and training models), Large language model (Access to a pre-trained LLM, which might involve cloud services like OpenAI's GPT or other equivalent models), Computational resources (Adequate CPU / GPU power for model training and inference), Data storage, Software development tools, Integration tools, Visualization and Reporting Tools

Data

Training data, Validation and test data, Real-world data, External data sources

Documentation and compliance

Legal documents, Compliance checklists, Ethics and bias evaluation

Testing

Performance metrics, User feedback mechanisms

Support and training

Training for end-users, Technical support.

Building a PoC for LLM in AFC is a significant undertaking that requires careful planning and the right resources.

Additional considerations

Sensa-NetReveal highlighted the importance of additional considerations including data and model validation.

Model development and training data

Gen AI solutions require exposure to vast amounts of data to produce the results they achieve

Model validation

Intensive testing for bias and hallucinations is a key component of the development process before a gen AI solution is deployed. Even with comprehensive training data, model biases can occur, as can hallucinogenic or 'made-up' responses. Developers mitigate these risks with appropriate reinforced machine learning and embeddings and human verification required

Transparency and interpretability

Unlike simpler machine learning models that follow a clear path of 'if-then' logic, gen AI models analyse many parameters and data points to form complex conclusions and produce nuanced outputs. Relevant explainability tools or models should be built into solutions

Security

One unique feature of gen AI solutions is the ability to input natural language prompts and to converse with the solution to achieve desired results effectively. Understanding if and how prompts and feedback might be used in the ongoing learning of the model is crucial, particularly in the AFC sector, where highly sensitive information is at stake. Ensuring a privately deployed instance of a model is used within a secure, firewalled environment and that prompts and inputs will not leak into the underlying foundational models should be top priorities.

LLM PoC in AML use-case

As this white-paper was getting ready for publishing, we interviewed senior AML Compliance and AML Compliance Analytics leaders from a global Bank headquartered in the UAE, that had recently concluded a PoC to evaluate if LLM can be used for more intelligence automated narrative generation. The results were noted as 'quite promising' although significant efforts are required to further ingest data for training, fine tune the models and improve hard ware.

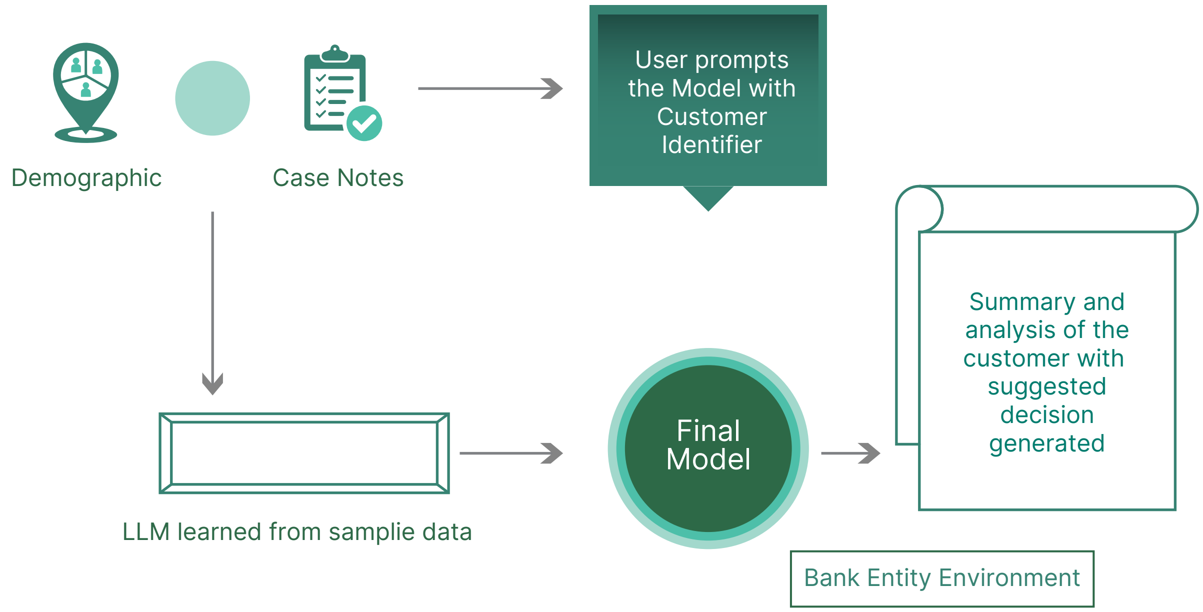
The following steps outline, at a high level, the processes followed:

Stage 1: Setting objective and outcome

Objective: Build a PoC using an LLM-based application for the Bank's AML Compliance with the ability to utilize multi-data formats to create summary, insights and propose decision for AML case investigations with a narrative

Stage 2: Ideation

High level summary of the ideation process:


Demographic
Case Notes
User prompts the Model with Customer Identifier
Summary and analysis of the customer with suggested decision generated
Final Model
LLM learned from sample data
Bank Entity Environment

POC ideation

Stage 3: Planning key steps

The team processed to assess multiple LLMs and finalised Meta Llama 7B LLM based in Azure cloud. Key steps:

Discovery	Security and privacy consideration	Interactive technical prerequisite	Environment setup	LLM Test
Ideation	Suggested approach by Information Security Team	Models	Theoretical vs practical learnings for LLMs	Design
Agreement	Within Entity Environment	Server/Instance	Optimized as per available resources	Build
Relationship building	No Internet connectivity	Experiment Feasibility, available infrastructure		Test

Stage 4: Execution of key steps

Execution steps

Environment and Components

- Initiated evaluation with a well known LLM with 7 Billion features, however, it required at least one 16 GPU machine (not split)
- Given lack of availability of single 16 GBU machine, the team chose Meta's LLama 7 Billion feature model with optimization (Quantization for less memory and computation in just one 8 GPU)

Security and Privacy

- All LLM, services and IDE (visual studio code - used for the development) were within Azure virtual machine with no internet connectivity

Key Libraries used

- Stream lit - for front end
- Lang chain - for back end
- C Transformer - for backend

Data Storage

- Data was stored in Azure blob with no internet connectivity

Data use

- Data extracted to MS Excel, with all PII (Personally Identifiable Information) masked

Static outcome

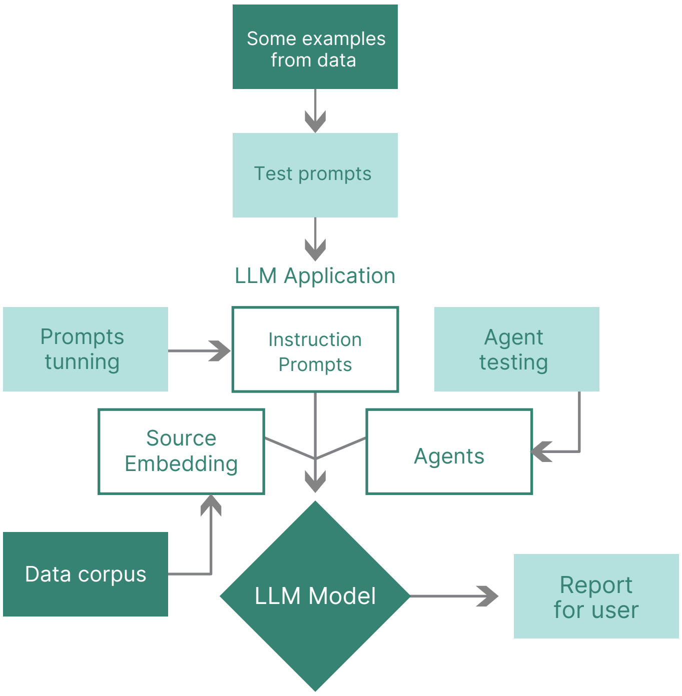
- Extracted non-cases files data through lookup logic in Python to get the static data

Generating the decision

- Case comments file used for few-shot learning and prompt engineering
- CSV converted to Json format - (Case comments)
- Json fed to LLM - parameters - as few shot learning
- LLM - understand the question and answer and produce answers using data set from this learning

Output

- Stream lit application is used for fetching the data and provide output
- In this code only the backend code fetches the data in the front end

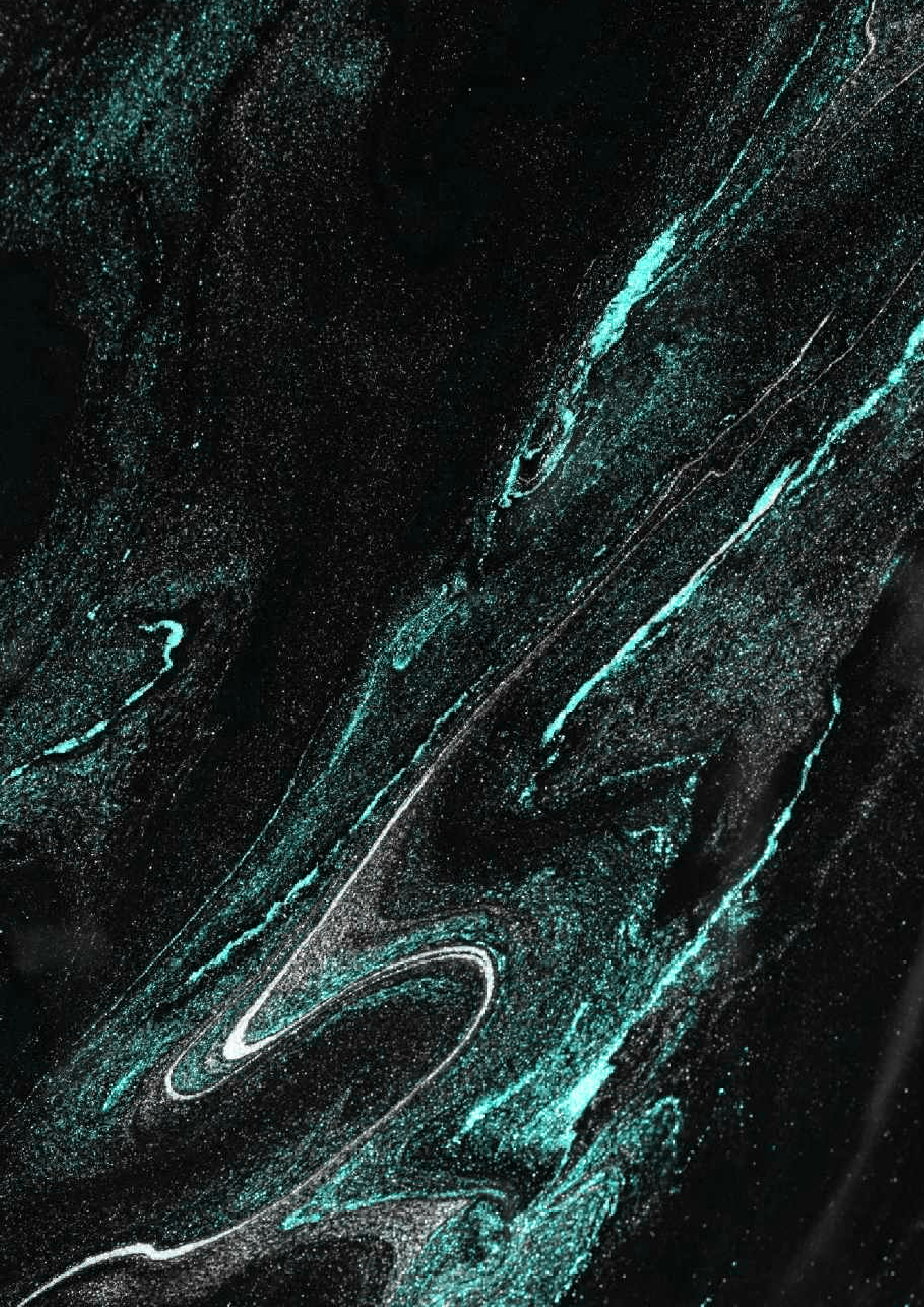


Key Libraries used

- Using Text Generation Inference (TGI) toolkit by HuggingFace to download, deploy model as API, and manage the scaling
- Model name: CodeLlama 7B - GGUF
- Model type: LLaMA (Large Language Model Meta AI) is a family of LLMs released by Meta AI starting in February 2023
- Input Models: Input text only
- Output Models: Generate text only
- Model Architecture Code Llama is an auto-regressive language model that uses an optimized transformer architecture
- Model Dates Code Llama and its variants have been trained between January 2023 and July 2023
- Using "ctransformer" library
- Helps load model in certain format like GGML or GGUF
- Library can pull support model from HuggingFace Hub
- Quantized model often require less VRAM than their original version, depend on the level of quantization
- This library is optimized with fast model loading to GPU.

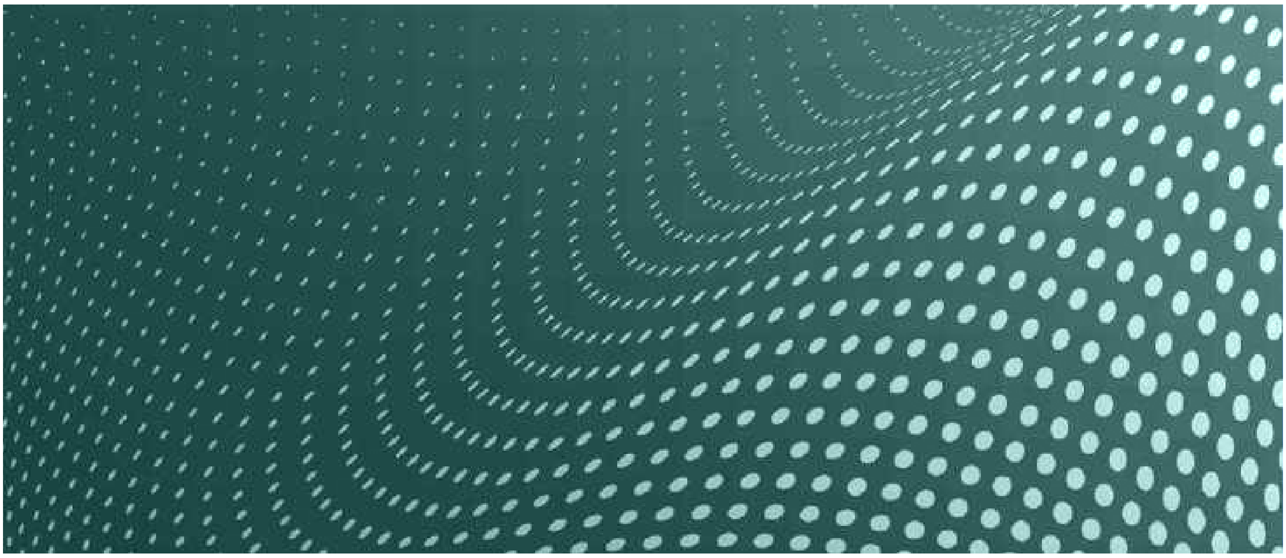
Conclusion

Large Language Models have undeniably the potential to transform the FI sector, providing innovative solutions and enhancing operational efficiency. With its comprehensive structure, real-time data processing capabilities, and innovative adaptation methods, LLM’s are paving the way for a new era, where data-driven insights and predictive analytics take front stage.



Section F

Core Models EWRA / FCRA, CRRM



Introduction

To successfully implement appropriate risk mitigation controls against money laundering and terrorist financing it is critical to identify, contextualise and measure risks. This requires an enterprise-wide risk assessment (EWRA) to understand the potential vulnerabilities within an organisation's operations. Most jurisdictions have established a robust legal framework that mandates organisations to conduct an EWRA to identify, assess, and mitigate the risks associated with money laundering and terrorist financing. This framework is based on international standards and best practice. To ensure an effective and efficient EWRA, organisations should consider adopting the following best practices:

- Establish a risk assessment framework
- Identify and assess money laundering and terrorist financing risks
- Implement risk mitigation measures.

While this is a critical activity, many organisations still use a predominantly manual approach to an EWRA, which involves:

- Data collection from multiple systems across the organisation
- Input of data into a risk calculator, typically excel based
- Aggregation of risks and risk measurements across various business units and/or jurisdictions
- Development of a risk assessment report to identify outcomes, key areas of concern and mitigation plan
- Ongoing monitoring of actions against risk mitigation plan.

During this largely manual process of conducting an EWRA, organisations often encounter various challenges that may hinder the effectiveness of the assessment. Some common challenges include:

- Data availability and quality
- Resource constraints
- Evolving regulatory environment
- Transparency.

Technology landscape

While technologies have been progressing at pace in areas like KYC through digital onboarding and transaction monitoring, there has been a slower pace of technology development to address the limitations

and challenges and to improve the effectiveness and efficiency of conducting an EWRA. The below will explore some possible options for technology advancement in this space.

Data collection is a critical activity in an EWRA and is often riddled with challenges and limitations, from data quality to inconsistency in data formats, to the ability to extract data from multiple systems across the organisation. Data collection during an EWRA also includes quantitative or statistical data and qualitative data through responses to targeted questions. Advancement in the automation of the data collection process through the development of a combination of API or ETL based data extraction and interactive and user-friendly surveys will add a significant level of efficiency and accuracy to the process. Furthermore, as the EWRA is a periodic exercise, the ability to pre-load and refresh previous assessment responses, while seemingly simple and obvious, does not widely exist today, yet can significantly add further value in managing the resource heavy nature of the exercise. Data collection is easily the most time-consuming activity of the EWRA process and is usually a key contributing factor to less frequent assessments. Automating this activity would help increase the frequency of this exercise and increase the quality and frequency of information about AML / CFT and sanctions risk exposure.

The main outcomes of the EWRA are the report and risk mitigation plan. An interactive dashboard style report with heatmaps, charts, and graphs provides great benefit to stakeholder who needs to understand the risk exposure across different dimensions and areas of the business. The ability to drill-down to a particular risk view to understand the drivers of the risk helps to quickly identify and mitigate risk.

Tracking progress and accountability of these actions is the next critical automation opportunity to enable active and deliberate risk mitigation outcomes and to ensure risk is detected and managed.

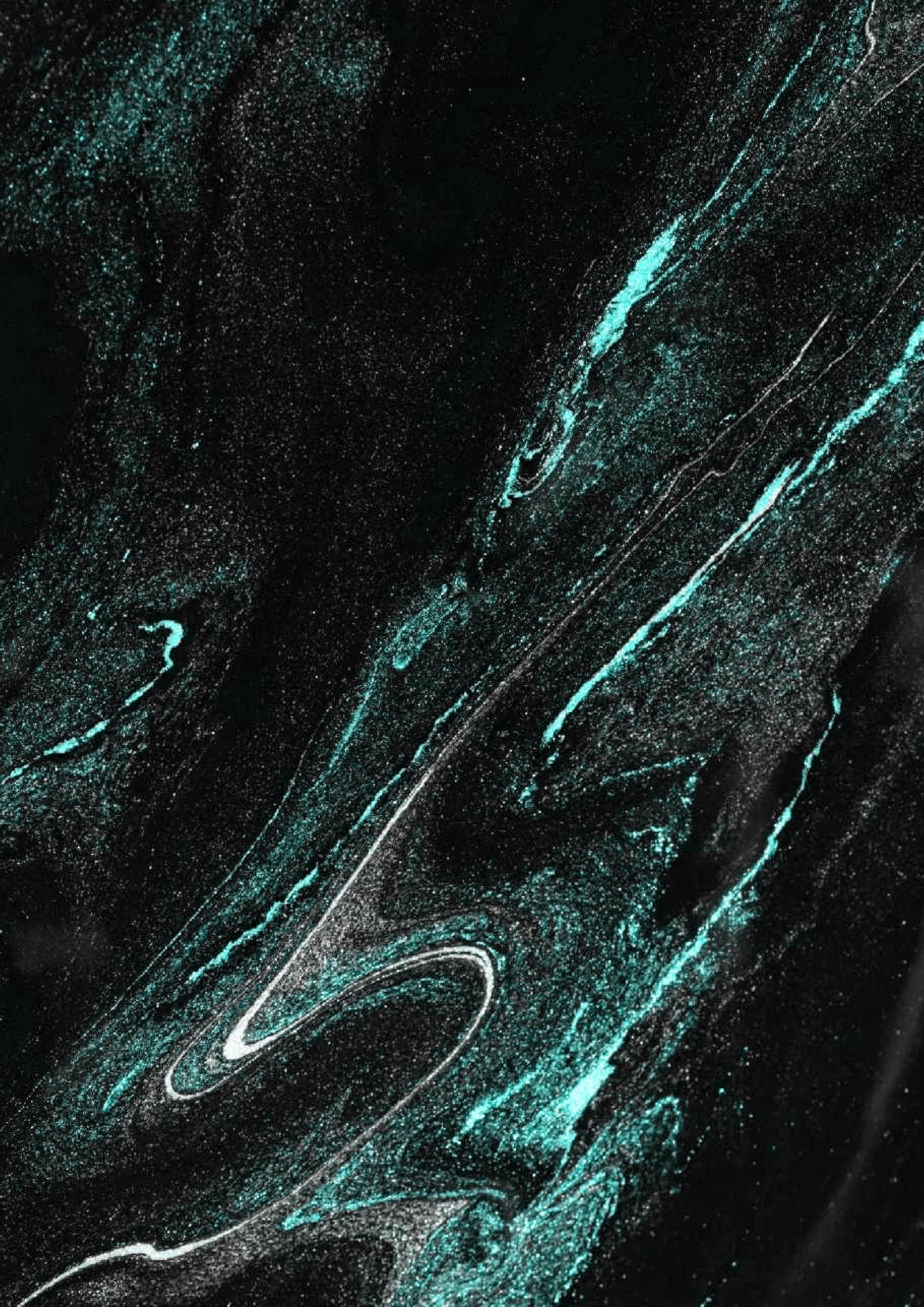
Now that the data is available and the risks are understood and managed, advanced technology can help predict risk. This is an innovative exercise not yet in use, but automation provides the ability to mine data to predict future risks and proactively plan risk mitigation actions.

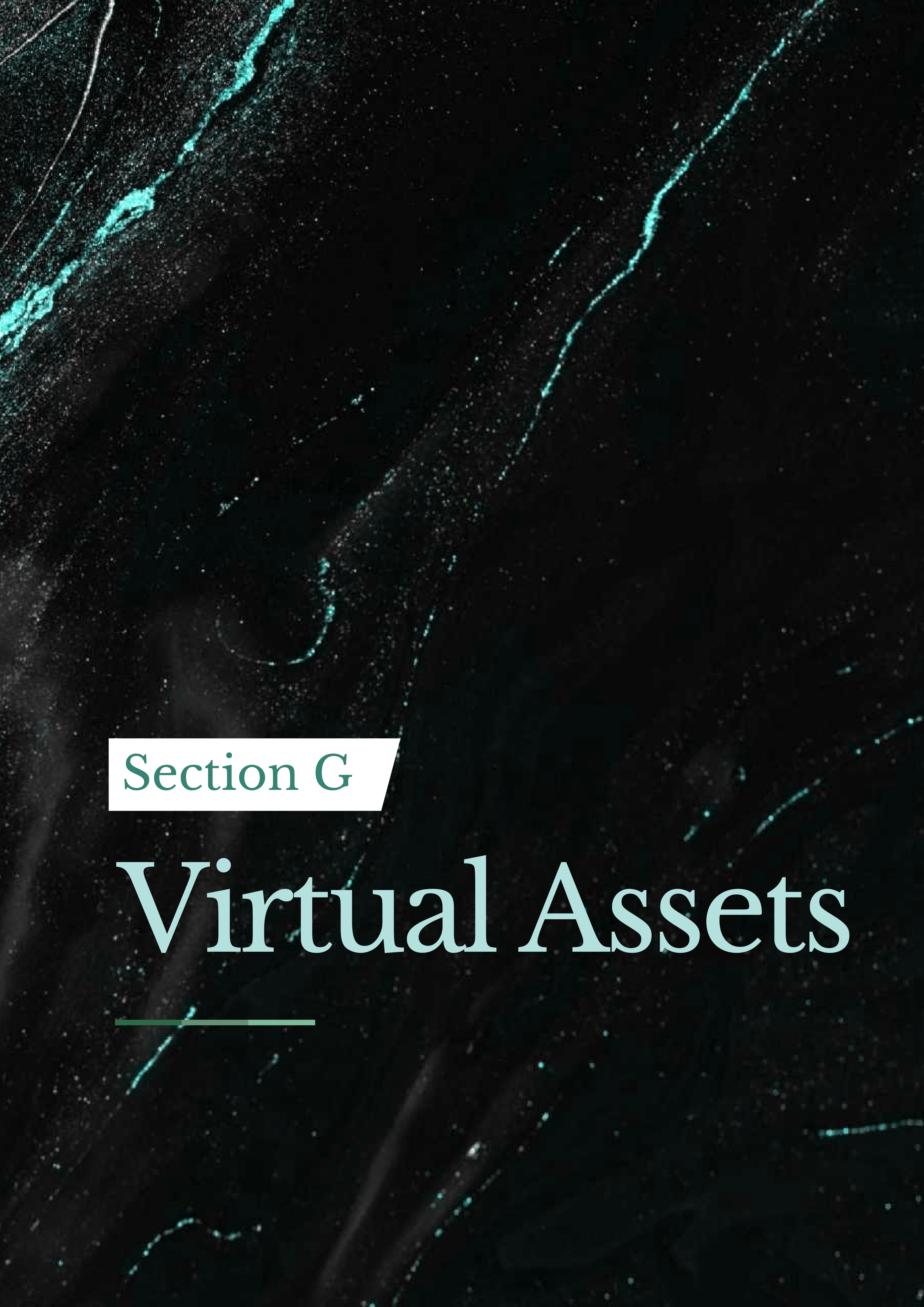
While a risk assessment framework is based on regulatory standards and global best practice, EWRA methodology is unique to each organisation and captures nuances that adds a layer of complexity when considering a technology solution. The solution, therefore, needs to have the ability to be both robust and

flexible. A more open architecture would enable easier customisation of the solution different risk factors, risk measurement, aggregation and calculation logic, reporting views and outcomes, for example, as well as the ability to consume data from multiple different source systems.

Conclusion

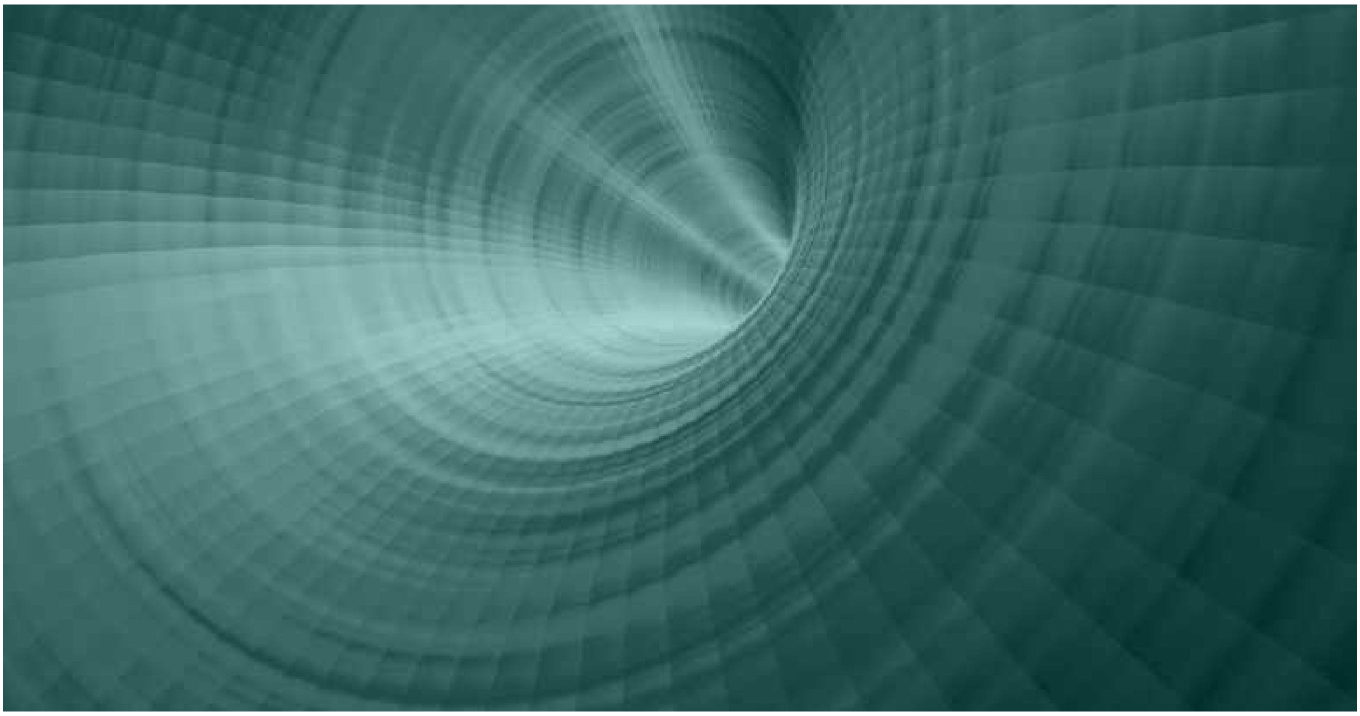
Conducting an enterprise-wide risk assessment for money laundering and terrorist financing is a crucial obligation for any regulated institution. By understanding the legislative requirements, adopting best practices, and addressing common challenges, businesses can effectively identify and mitigate the risks associated with financial crimes, ultimately contributing to a more secure and resilient financial system. Although technology may not be the “silver bullet” that is needed to complete a thorough and robust EWRA at this stage, it will support a more efficient, complete, and accurate EWRA process and provide an online, ongoing and transparent view of the organisations’ risks to assist to prevent ML and TF.





Section G

Virtual Assets



Virtual Assets

A tectonic shift in the virtual assets ecosystem is well and truly underway in 2023. As the world waits for regulatory clarity on virtual assets from governments, there is increasing opportunity for the UAE Government to implement an open regulatory framework and become the centre for development in the years ahead.

The innovation of representing and transferring value on a blockchain has potential to provide transparency in transactions and efficiency in settlement. At the same time, the ease with which virtual assets can be monetised, transferred and exchanged comes with risks, particularly with financial crime.

Globally, in line with the recommendations of global standard-setting bodies such as the Financial Action Task Force (FATF), regulators are working on an approach to virtual assets to combat financial crime risk. In this regard, developments in blockchain analytics have been key in helping regulators and virtual asset service providers (VASPs) overcome such risks. Whilst the focus of this paper is on technology, not regulation, the two are inextricably linked. and through the course of the interviews we held with industry experts, a clear theme emerged when talking about the potential for the development of technology and the sector in general, and that was the creation of an optimum regulatory environment.

Technology vs regulatory oversight

The open nature of blockchain transactions lends itself to financial crime detection models and reporting that could surmount some of the inefficiencies and silos in the fiat world. There is, however, a consensus amongst our experts that the capabilities of blockchain analytics for financial crime risk management should be better utilised.

Esteban Castano, CEO of TRM Labs, highlights the challenge for technological development in the virtual assets space. *"The time scales of technology development and regulatory evolution are inherently out of sync. Technology evolves on a daily basis and regulation does not".*

Amit Sharma, CEO of FinClusive, agrees: *"Innovation in the sector is always going to outpace regulatory oversight. The good news is that the tooling to monitor, track, trace and interdict potential illicit transactions benefits from some of the underlying attributes that blockchain technologies afford - which are the underpinnings of digital assets themselves".*

However, the growth in traditional finance organisations as they begin managing direct and indirect exposure to virtual assets may drive maturity in this area.

David Carlisle, Vice President of Policy and Regulatory Affairs at Elliptic commented, *"Blockchain analytics may evolve as more TradFi firms come to utilise it, who have much more complex regulatory requirements than typical VASPs, but also have much more complex tech stacks"*.

Mr Carlisle foresees that traditional finance houses will eventually incorporate virtual asset analytics in their risk management systems: *"TradFi firms will be integrating some component of crypto-related risk identification into their transaction monitoring capabilities"*.

The potential integration of blockchain analytics technology with existing financial crime technology is very interesting. Much work must be done to ensure old and new technology complement rather than complicate each other.

Legacy approach to technology

There is a sense among our experts that financial crime technology depends too much on legacy methods.

Michael Mosier, Ex-Head of FinCEN, believes it is time for an innovative approach. *"We are still stuck in basic documentary validation, over indexing and focusing on collection of a document when there are many other data points that can be used."*

Asaf Meir, Co-founder and CEO of Solidus Labs, agrees: *"Artificial general intelligence could revolutionise the way compliance is managed, focusing on behavioural-based risk monitoring rather than identity-based risk monitoring as it relates to the detection of market manipulation. Also important to keep in mind – AI trading bots both in crypto and TradFi are already showing early signs of deploying trading tactics, which could result in market abuse. The only truly effective way to combat that would be to employ AI tools for detection - which goes back to focusing on trading behaviour vs. identity"*.

Mr Mosier added, *"The ability to trace transaction activity indefinitely, in a way that creates meaningful attribution linked to data lakes and analytics, is leading to a scenario harder to spoof than identity-based risk analysis like document evidence or a shell company. Work is being done to connect on- and off-chain, to link entities and individuals to wallets though off-chain activities, which is more effective than static document collection."*

Big data and analytics were strong themes throughout our conversations with our experts. There was a shared impression that the technological capabilities to advance in this space are there and that this is an area where we expect exciting developments in the near future. Data growth has been exponential in recent years, but more exciting is the acceleration in computational speed and analytic capabilities. These powerful capabilities can unlock the true potential of advanced analytics in financial crime risk management.

With the bridging of the traditional financial crime 'off-chain' data universe and the growing 'on-chain' data world in the virtual assets space, there is a belief that this will result in impressive intelligence lead technology that will offer incredible capability to the industry.

Privacy preserving technology

One of the areas our experts are most optimistic about is privacy preserving technologies. **Pascal Aerens**, Co-Founder of Neterium, sees the rise of programmatic privacy as one of the most exciting developments. *"Privacy was either on or off. You're either Bitcoin and everything's transparent, or everything's private and where we're heading is that you have programmable privacy at the protocol layer, at the middleware layer and at the application layer. That gives developers the ability to fine tune controls to protect financial privacy while enabling AML objectives."*

Capabilities like Zero Knowledge Proofs (ZKPs), which can now be executed in real-time, open an opportunity to break some of the barriers that data privacy legislation has brought to the financial crime risk management sector.

"You are going to see increasing numbers of privacy preserving KYC providers who just confirm someone is not from a high-risk jurisdiction or on a blacklist rather than providing full identifier information," **Mr Mosier** believes. *"The potential to use ZKPs to prove someone going into a pool is not sanctioned or similar – that's meaningful risk reduction"*.

"Technology today allows us to share information but still keep it protected", **Mr Sharma** added. This is particularly interesting in the virtual assets space, where digital identification is the norm, and many projects are underway to bring the potential of identity passporting to more mainstream use. This is particularly interesting in the UAE, where there is the potential to use ZKPs to address regulatory challenges to data localisation. The reality is that many of the most exciting developments in the FinTech space are occurring in cloud native environments, which can create data localisation challenges. But privacy by design concepts, including ZKPs, allows for design solutions to navigate those obstacles. They also open a gateway to faster technology adoption in the UAE and other markets operating with similar regulatory frameworks. Regulation is one of many drivers here. Consumers are increasingly aware of the need to control and take ownership of their data, especially identity data. We expect to see exciting developments related to identity data provisioning in a more advanced data-sharing model. Advanced data-sharing capability will lend itself very well to markets with strong national identity programmes, often limited to domestic plays rather than global solutions.

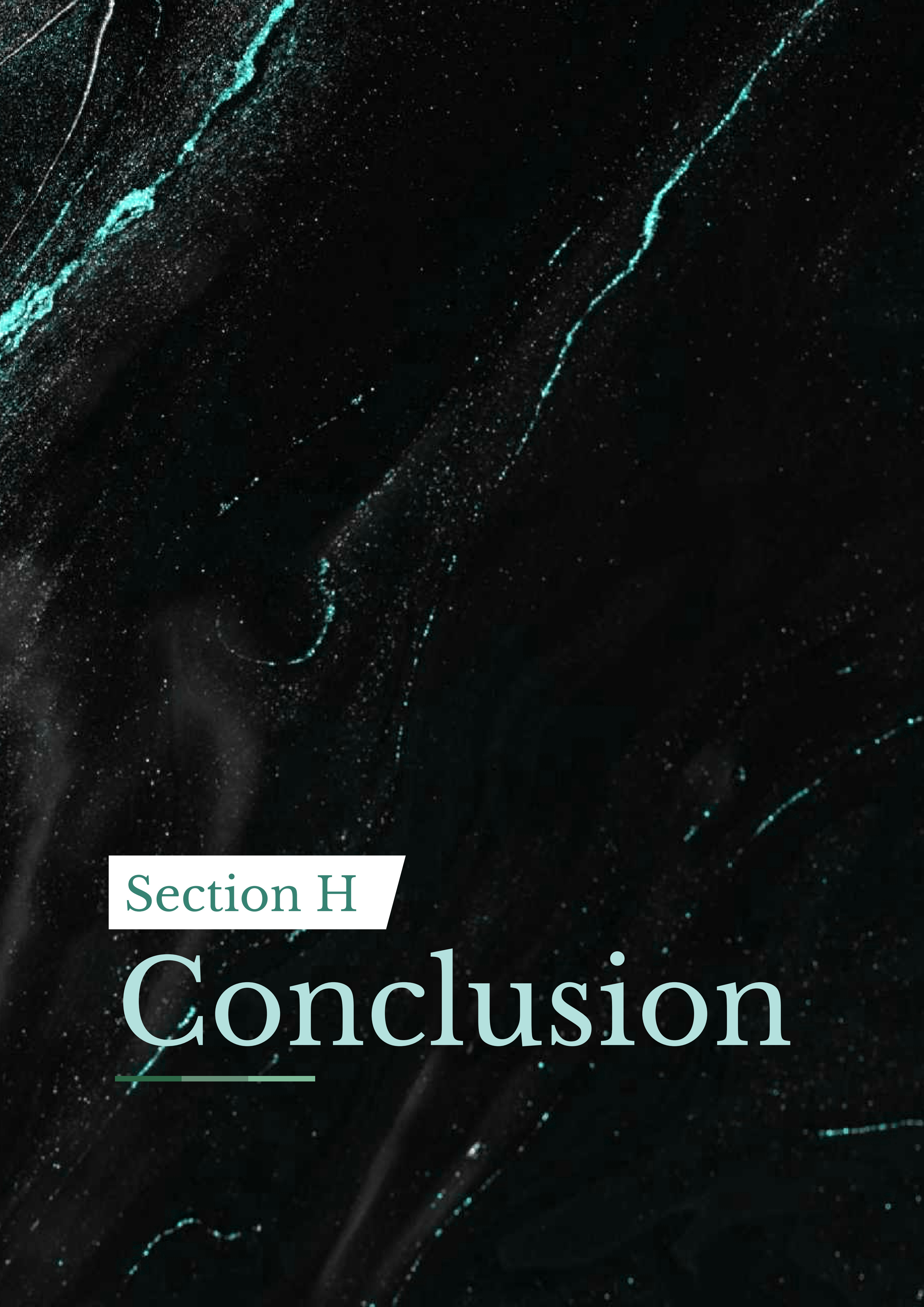
Looking ahead

The virtual assets industry can drive technological advances, delivering benefits and application far beyond the distributed ledger technology environment.

The level of innovation and the speed of growth in this sector means it is highly likely that technological developments will outstrip the pace of development in traditional environments. Experts are optimistic that we are about to enter a stage of meaningful technological development in financial crime risk management.

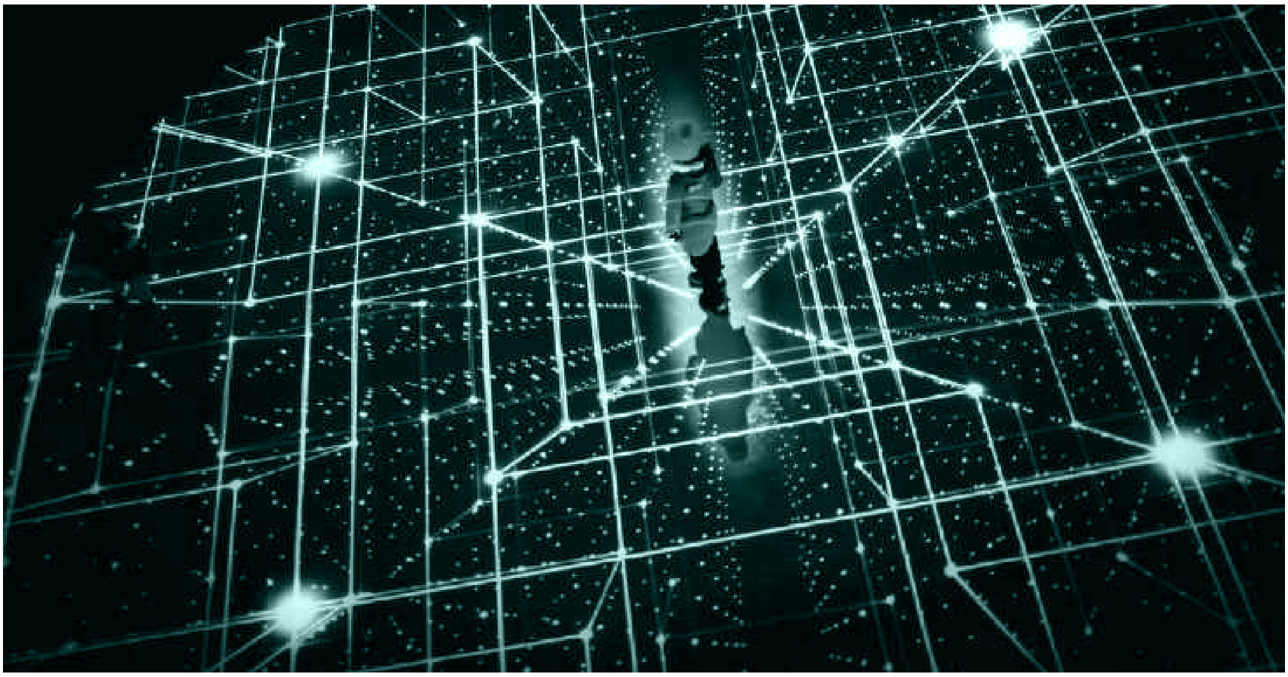
To get there, however, will require a mix of forward-looking, open-minded regulators who provide the right environment to allow this development to flourish. A progressive regulatory environment will support intelligent technology development able to navigate an increasingly fragmented global regulatory landscape while truly bridging the gap between the on and off-chain universes.

"I think in our business if you stay still for six months, your product expires. The surface area of crypto is expanding so rapidly that it just requires constant technology innovation," said **Mr Castano**.



Section H

Conclusion



There is no argument that the anti financial crime community stands at a point in time where the opportunities thrown up by advanced technology are the greatest compared to any time in recent history. However, there are multiple challenges to surmount and at the core is talent. The ability of compliance and anti financial crime professionals to upskill and learn the language of technology so that conversations with their peers in the data, tech, analytics and digital world are more meaningful and reap the benefits of what the future has to offer.

Mr Choi, concludes, *"It's challenging to find practitioners with both the technical data science skills and SME expertise in AFC which are necessary to adopt advanced AI-based solutions. You need to be able to design and implement the technology as well as explain in plain language how the new technology improves the FI's financial crime risk management which is the ultimate objective. FIs have tried to build collaboration with AFC SMEs and data scientists but this has been more challenging during pandemic and remote/hybrid work. And as always, data remains one of the biggest challenges to implement more advanced solutions effectively".*

However, for any organisation to make remarkable improvements, as always, culture, and tone at the top is critical. Especially for traditionally non-technical departments like Compliance, a shift in mind-set is key to make progress. **Mr Hills** highlights *"Organisations don't consider the importance of fostering a Digital culture enough. Not everyone understands the importance of living and breathing a tech / data mindset".*

Ignoring the changing landscape or maintain inertia is not an option for AFC professionals. *"We in the Compliance industry are at a tipping point of building and deploying technology to manage compliance risk. But we have to overcome the mindset that not all that we did yesterday that got us to this point, is going to work for tomorrows problems, especially with the speed at which our customers change and subsequent exponential growth in data points to review. To better prevent, detect, and mitigate financial crime risk we need to have in our toolkit technology that can collect, analyze, and suggest the way forward over large data sets. Organizations may still be able to manage its risks using current rule based methods, but sooner or later your space will be taken by someone who has successfully made that step"*, notes **Scott Ramsay**, Group Head of Compliance and Bank MLRO at Mashreq Bank.

Future Anti Financial Crime model and skills

To keep pace with changes in technology, it is clear that the hitherto non-technical Compliance officers have to upskill – at pace. Laying the roadmap for upskilling their teams must be a key priority for leaders and managers. The future AFC teams may be divided primarily in to three groups of skills:

Risk Analysts

Analysts expert in understanding financial crime risk, typologies, controls and mitigation, trained and skilled with at least an elementary, but hands-on knowledge of Data, Analytics, Machine Learning models and AI

Risk Engineers

Engineers, Data Scientists with deep experience in data, Cloud computing, building, testing and running advanced risk-mitigation models and skilled with at least and elementary, but hands-on knowledge of financial crime risk

Leadership, SME and Interlocutors

The Interlocutors shall be individuals highly skilled in both domains i.e. Risk Analysis and Risk Engineering

Needless to say, collaboration is the key to strong outcomes. A digital mind-set, the ability to see the opportunity of building controls in a preventive, in-built design at product level, fostering strong relationship with Business and Digital teams and scientific temper will go a long way in transforming AFC units and prepare them for the future.

"The complexity of the modern world calls for sophisticated tools to attend to the fight of financial crimes in an efficient and effective manner. Leveraging advanced technology and analytics has become more vital than ever to build a sustainable and resilient framework to identify suspicious activities and enable swift and timely reporting", notes **Rasha Mortada**, Group Chief Compliance Officer, Abu Dhabi Commercial Bank

"The use of AI in fighting financial crime presents us with the opportunity to dramatically improve effectiveness and not just efficiency. AI to be truly effective though must learn from lots of human intelligence based as much on known criminal activity and not just suspicion or unusuality. This requires both public and private sectors to work together, prioritise and be selective on the data that is used to educate the systems of the future and have controls to ensure the models we make are models we all can trust", reflects **John Cusack**, previously Global Head of Financial Crime, Standard Chartered Bank and Chair of the Global Coalition for Fighting Financial Crime.

Appendix

Appendix 1: pKYC risk drivers, sub-categories

Risk Drivers & Behaviours	**Sub-Category**	**Description (calculated based on historical data statistical analysis)**
Overall		
Cash Parameters	Cash deposits - Branch, ATM machines/ kiosks	% of total cash deposits compared to sum total of credits in the account
	Cash deposited by third parties	% of cash deposits by third parties compared to total cash deposits. ' Third parties' here includes any persons other than usual third parties.
	Cash withdrawals internationally	% of cash withdrawals by value made internationally, to the total debits in the account
	ATM deposits as % of Total Credits	% of cash deposits at ATM, to the total credits in the account
Retail		
Non-Cash (Except International Wires) Parameters	Credit cards/POS used divided by total debit from the account	% of credit cards/POS transactions (by value) to sum total of all debits from the account
	Total cheques deposited	% of cheques deposits compared to sum total of all credits to the account
Remittances Parameters	International remittances - Incoming (Value)	Value of incoming/inward international remittances compared to sum total of credits to the account
	International remittances - Incoming (Volume)	Total count of incoming/inward international remittance transactions compared to the total count of credit transactions to the account
	International remittances - Incoming from High-Risk Countries	Whether any inward remittances have taken place in the customer's account by a payer from a high-risk country
	International remittances - Outgoing (Value)	Value of outgoing international remittances compared to the sum total of debits from the account
	International remittances - Outgoing (Volume)	Total count of outgoing international remittance transactions compared to the total count of debit transactions to the account

Risk Drivers & Behaviours	Sub-Category	Description (calculated based on historical data statistical analysis)
	International remittances - Outgoing to High-Risk Countries	Whether any outward remittances have been made to a receiver in a high-risk country
	Foreign Currency Deposits	Where the customer has deposited foreign currency, the value of such currency compared to the sum total of total credits to the account
	Foreign Currency Withdrawals	Where the customer has withdrawn foreign currency, the value of such currency compared to the sum total of total debits from the account
Overall Account Activities	Actual deposits in comparison to expected deposits	The parameter considers the customer's actual credits when compared to expected credits as declared at the time of onboarding
Other Customer Behavioural Parameters	Total number of high-risk products held by the customer	the higher the number of products held by the customer, higher is the probability of ML/TF risk involved.
	Number of static data change requests	KYC update request sent by the customer to notify the bank of changes in personal details. Updates to any of the following would constitute static data changes - 1. Residential or correspondence address 2. Email ID 3. Contact number
	Continuous periods of inactivity	Duration between two transactions to track any period of inactivity in the account
	Number of supplementary cards issued to an account	Where the customer holds any cards (debit, credit, prepaid, travel, etc.) and has added supplementary cardholders to the account
Corporate		
Triggers for corporate customer		• Reincorporation or change of locations • New shareholders added • Changes to the board or shareholders • Multiple changes to senior management in a short period

Title: Current Views on Technologies in Anti-Financial Crime

Compiled by: Digital Working Group of the AML/CFT Partnership Forum, a Public-Private Partnership platform set up under the Executive Office of the Anti-Money Laundering and Counter Terrorism Financing in the United Arab Emirates.

Disclaimer: Despite the careful efforts made by DWG to prevent errors or omissions in this document, any unintentional mistakes or omissions are not intended. The information presented herein is solely for reference, educational, and awareness purposes and is subject to change without notice. It is important to acknowledge that DWG or any affiliates cannot be held responsible for any damage, loss, or other consequences arising from activities undertaken based on the information provided in this document.

Languages: English

Number of pages: 75

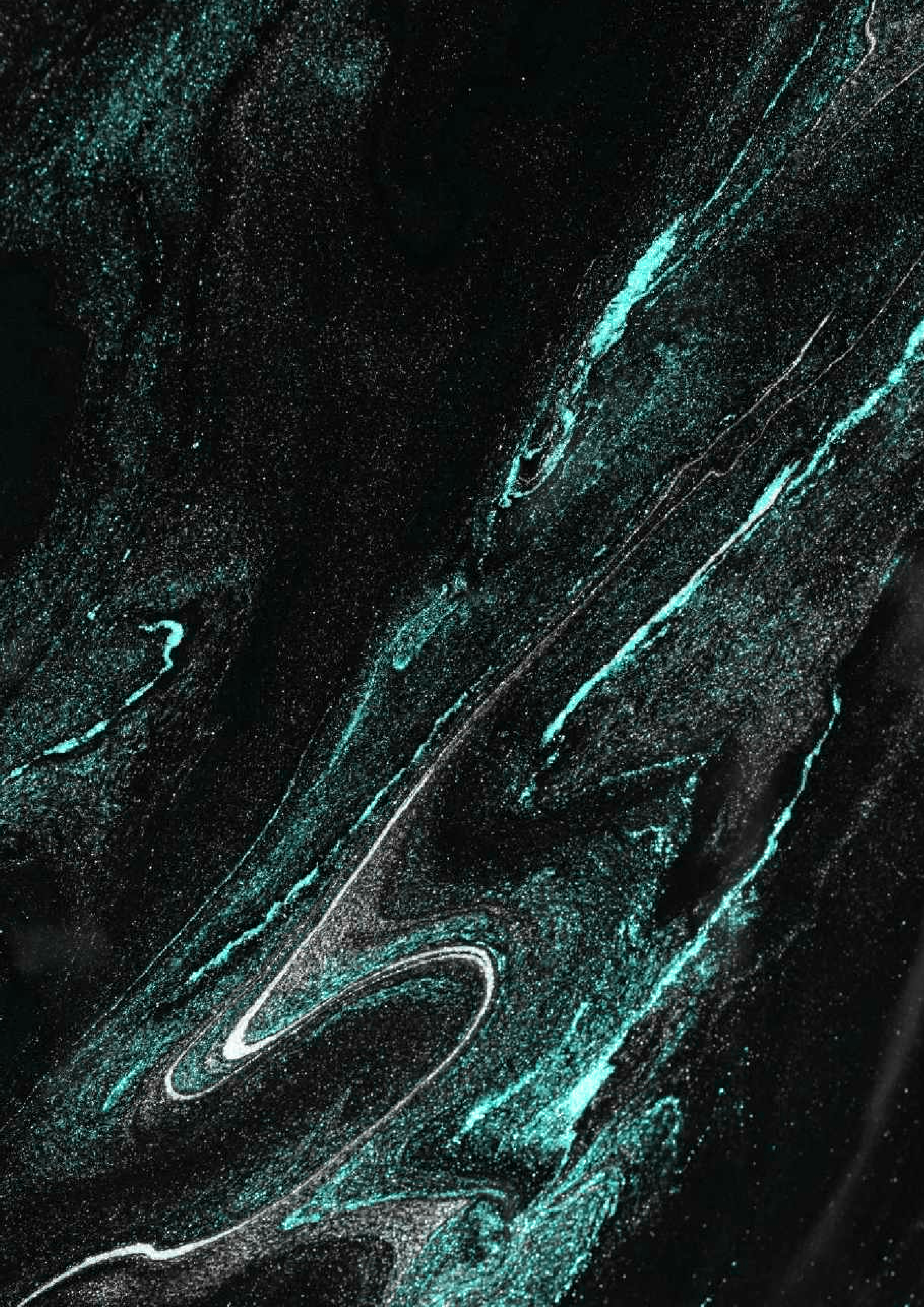
Edition: 1st edition

Month and year of publication: Feb 2024

Endorsed by:

MENA FCCG
Making a Collective Impact

This document is not for sale. This document shall be distributed by Digital Working Group of the AML/CFT Partnership Forum, a Public-Private Partnership platform set up under the Executive Office of the Anti-Money Laundering and Counter Terrorism Financing in the United Arab Emirates or their affiliates to individuals and entities as they deem fit.



منتدى الشراكة في مواجهة غسل الأموال
وتمويل الإرهاب
AML/CFT Partnership Forum