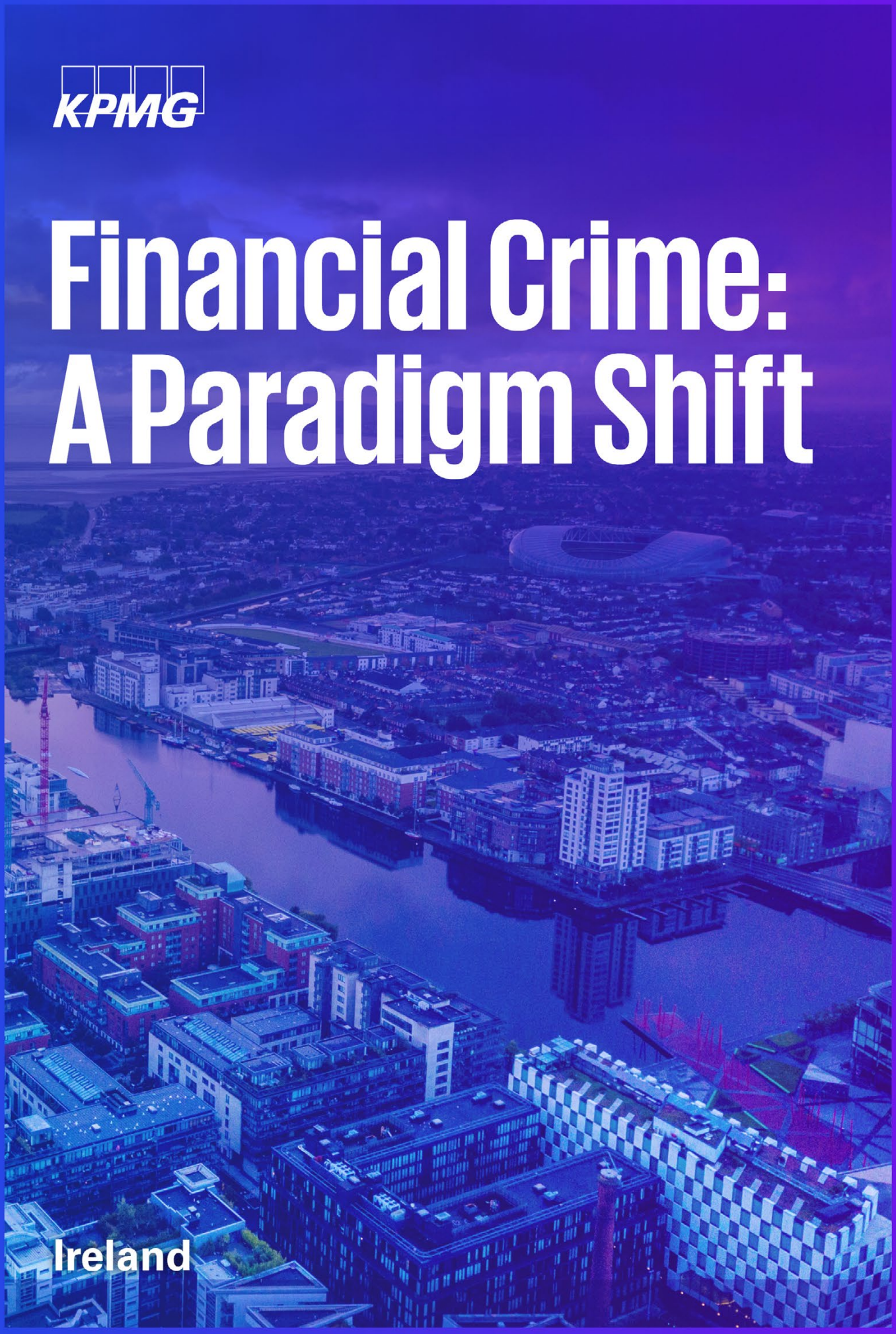
KPMG

Financial Crime: A Paradigm Shift



Ireland

CONTENTS

FOREWARD: NIAMH LAMBE

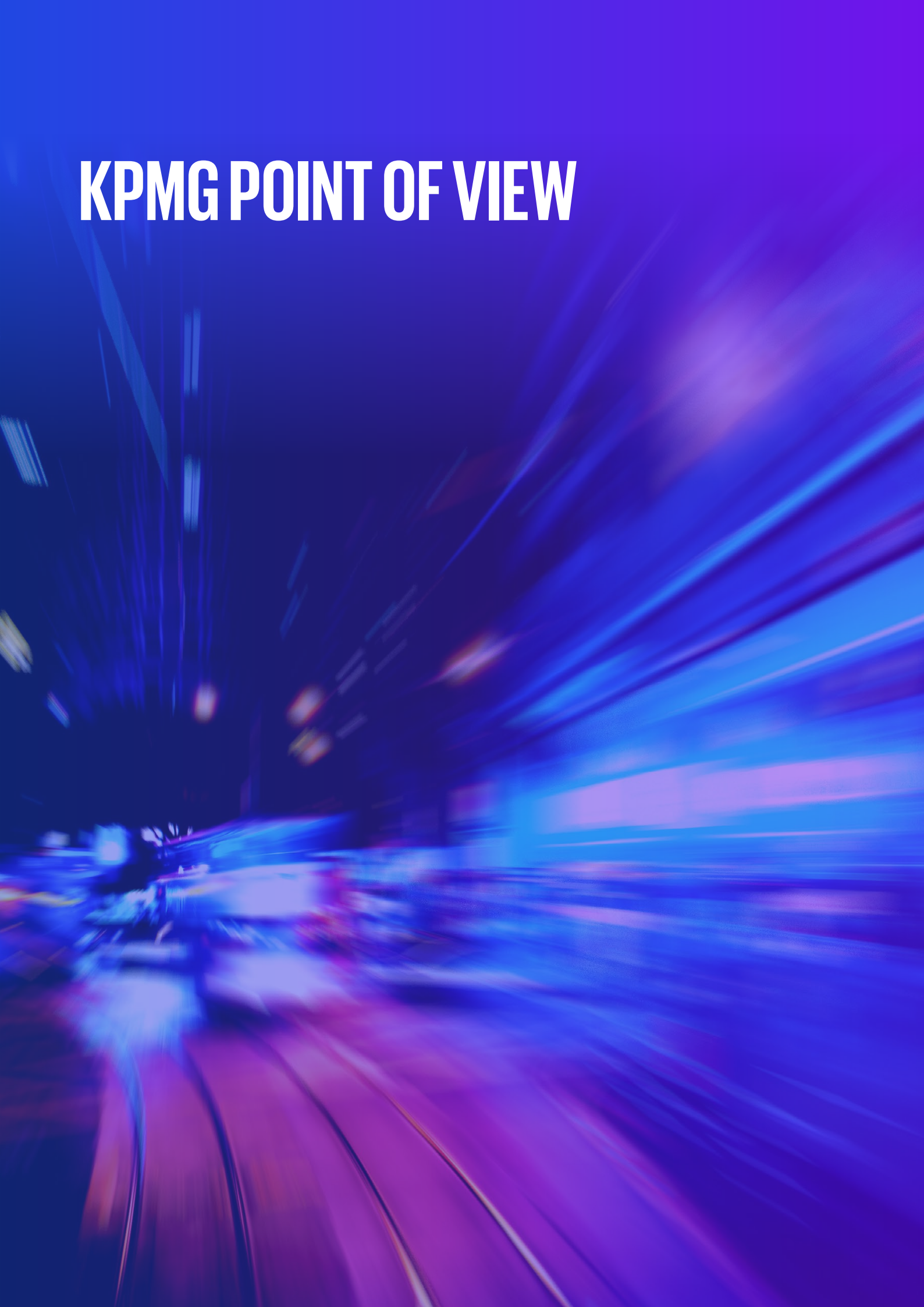
Criminal activity is becoming increasingly sophisticated with the use of new and emerging technologies to exploit financial systems. More than ever, we need financial institutions that are equipped to play a critical role in preventing, detecting, and deterring crime.

With evolving financial crime threats and heightened regulatory scrutiny, firms are reassessing their approach to financial crime risk management and compliance, and are paying a heavy financial cost, collectively spending billions trying to prevent financial crime. And so, maturing and embedding a robust FinCrime operating model to meet regulators expectation, without adding cost, is becoming critical to driving strong regulatory outcomes.

In this context, we are sharing with you our view of a 'Paradigm Shift' in the approach to Financial Crime. Based on interviews with 16 global thought leaders, from industry, government, RegTech, law enforcement, consulting, and academia we consider where the journey in combatting financial crime will lead, and the paradigm shift needed to get there; we identify 6 major trends that we anticipate will shift the paradigm of disrupting financial crime compliance over the next 5 – 10 years, followed by 6 practical calls to action that organisations can take to better combat financial crime, innovating with data and technology to manage costs while meeting regulatory expectations.

Niamh Lambe
Managing Director
Head of Financial Crime
KPMG Ireland.

KPMG POINT OF VIEW



KPMG POINT OF VIEW

Six major trends that we anticipate will shift the paradigm of disrupting financial crime compliance:

THE PARADIGM SHIFT

01 FINANCIAL CRIME COMPLIANCE WILL BE PURPOSE-LED

Drive effective outcomes by being purpose-led – disrupting criminal activity for the good of the organisation, customers, and our community.

02 EFFECTIVENESS RATHER THAN TICK BOX COMPLIANCE

Define what success looks like, with flexibility to focus on agreed threats under a risk-based approach.

03 DEEPER PUBLIC-PRIVATE PARTNERSHIPS

Deliver greater results and disruption of criminals through strategic data sharing using PPS.

04 NEW WAYS TO KNOW YOUR CUSTOMER

KYC and CDD remain a core pillar, with shifts towards perpetual-KYC and data-driven real time monitoring.

05 NEXT-GENERATION FINANCIAL CRIME DETECTION SYSTEMS

Deployment of machine learning and artificial intelligence for complex decision making.

06 DATA AND TECHNOLOGY WILL UNDERPIN THE FINANCIAL CRIME COMPLIANCE EVOLUTION

Complete, accurate and timely data, with integrated technology solutions supported by a clear strategy.

In many organisations the expected paradigm shift will require large-scale transformation and commitment, smaller organisations can also leverage the shift away from "tick box" compliance and drive a proportionate risk focused model. This evolution must begin now. Our research has identified six practical steps that organisations can take to better combat financial crime:

CALL TO ACTION

01 FIX, REMEDIATE, BUT DON'T LOSE FOCUS ON THE STRATEGIC

Define a target state operating model that enables teams to act tactically while thinking strategically.

02 MOVE TO PERPETUAL KYC

Digitise the KYC process to improve data quality, enhance compliance, and improve outcomes.

03 INNOVATE CUSTOMER MONITORING, STARTING WITH COMPLEX ML/TF

Augment rules-based engines with intelligence-led analytics tools that target complex and intelligent scenarios.

04 FIX YOUR DATA TODAY, BUT DON'T WAIT FOR IT TO BE PERFECT

Data aggregation can accelerate effective financial crime systems but know that data does not have to be perfect.

05 ALIGN TRANSFORMATION TO A STRATEGIC PLAN AND CONTINUE TO INNOVATE

Transformation is a continuous journey and should not be locked into a fixed timeframe.

06 EMPOWER FINANCIAL CRIME OPERATIONS

Financial crime operations teams are key to improving effectiveness and efficiency.

FIND OUT MORE

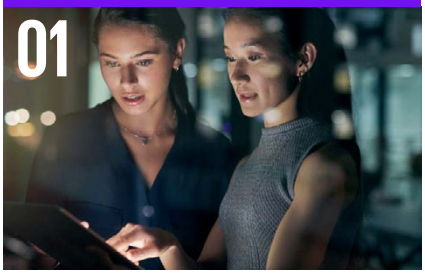
FIND OUT MORE

The financial crime paradigm shift will be an evolution:

The thought leaders featured in this publication have clear visions for the future in the fight against financial crime.

We see this as more of an evolution rather than a revolution as advancements will take place over time, and at different speeds depending on the organisation.

This is our view on the evolution that we expect to see over the next 5 – 10 years:



Financial crime compliance will be purpose-led

To contribute actively to combatting crime, financial institutions will drive effective financial crime compliance outcomes by being purpose-led. This means that institutions will need to focus on the spirit of financial crime compliance laws – preventing criminals from having anonymous access to the financial system and providing actionable intelligence to law enforcement to disrupt criminal activity for the good of the community and society. Driving change and embedding a strong compliance culture in financial institutions will require clear communication on what an institution is trying to achieve. When done right, the long lasting benefits are huge, to the organisation, to its people, to its customers and the community.

The focus will be on effectiveness rather than 'tick box' compliance

The focus on effectiveness in financial crime risk will increase. Some regulators and financial institutions have begun to move away from the 'tick box' technical compliance mentality; a change kickstarted by the effectiveness assessment approach of the Financial Action Task Force (FATF) and now being implemented at a national level.

The focus on outcomes rather than outputs in financial crime compliance will significantly increase over the next 10 years. Policies and procedures must adapt to enhance the effectiveness of vulnerable entities in preventing financial crime exploitation in their sphere of influence. Financial institutions will need to define what success looks like to remain outcome focused using a risk based approach.

There is an opportunity for regulators and the industry to work closely together to agree on what the desired outcomes should be and allow some flexibility to focus on agreed threats under a risk-based approach.

Deeper Public-Private Partnerships through data sharing

Public-Private Partnerships (PPPs) are the future, and there is an opportunity to grow their operational value.

There has been a dramatic increase around the globe in the prevalence of PPPs designed to directly combat financial crime. These partnerships have been an effective way for organisations to share information on focus areas, criminal threats, and typologies.

Operationally focused PPPs have delivered promising results. This trend will likely continue as financial intelligence units (FIUs), law enforcement, and national security agencies start to see the value of working with financial institutions at a tactical level.

The future will be intelligence-led collaboration between financial institutions. This presents challenges but will be critical to protecting the entire financial system, society, and our communities.

FIND OUT MORE

There will be new ways to Know Your Customer

Know Your Customer (KYC) and Customer Due Diligence (CDD) will continue to be central to both compliance and core business process. Financial institutions have invested heavily in KYC upgrades in recent years. However, many continue to struggle with inefficient and ineffective implementation due to cumbersome processes and procedures, fragmented data, and labour-intensive operations. Chronic underinvestment in critical functions such as data aggregation has prevented companies from generating the insights they need to effectively combat modern criminals. This will need to change.

Over the next 10 years, there will be a significant shift in the execution of KYC due to advances in technology coupled with enhancements in data. The digitisation of KYC will be supported by the automation of key processes. Customer onboarding will be overhauled to focus on each customer's potential financial crime threat, rather than today's binary risk allocations based on broad factors which do not consider evolving complexities and nuanced risk.

Ongoing CDD will move away from static periodic reviews to datadriven, real-time monitoring based on customer risk. This will provide a deeper knowledge of who these customers are for better risk-based decisioning. Ultimately, a new approach to KYC must reduce risk, improve customer experience, and reduce costs in the long run.

Next-generation financial crime detection systems

Financial crime detection systems will evolve dramatically over the next 10 years. Many institutions are currently struggling under high ratios of false positive alerts, and the ratio is worsening. The next generation of detection tools will be more dynamic and use intelligence to assess real threats and produce higher value alerts for investigation. We expect to see a rapid increase in the deployment of machine learning and artificial intelligence for financial crime detection. This will start with the use of machine learning in the first-level classification of alerts and rule hibernation, before moving to the use of machine learning and artificial intelligence in more complex decision making.

This will result in earlier flagging of higher value cases, with less time spent reviewing false-positive alerts so that financial institutions can better target investigations.

Data and technology will underpin the financial crime compliance evolution

A common thread in all our interviews was the importance of the data that underpins all financial crime compliance. The data collected on customers and their behaviour will continue to expand at a rapid rate. But it is not just enough to just have the data, it needs to be aggregated and structured in a way that can be leveraged for intelligence gathering and investigation. This does not mean data needs to be perfect. There are several tools that are already demonstrating what can be achieved with less than perfect data.

By utilising complete, accurate, and timely data, financial institutions can more effectively analyse financial crime threats and activity. Good data governance and risk-based approaches to data lineage will provide a pathway to complete, accurate and timely data.

Financial institutions will also look to move away from disjointed technology systems to an integrated solution supported by strategy.

The automation of case management activities will grow, relieving analysts to allocate more time to analysis rather than the collation of information.

It will be critical that financial institutions get their operating models and processes right before implementing technology, otherwise, financial institutions risk simply making a poor process faster.

CALL TO ACTION

CALL TO ACTION

While some of these changes seem a long way in the future, the good news is that financial institutions can start now. We have highlighted 6 calls to action that financial institutions can consider now to better combat financial crime:

01

Fix and remediate, but don't lose focus on the strategic

Financial crime transformation requires a balance of acting tactically while thinking strategically. Financial institutions need to first define their target state, so that they can address their immediate issues in a way that aligns with their future strategy.

This starts with getting the foundations right to manage financial crime risk, such as developing a strong culture of compliance, establishing a target operating model that is fit for purpose, and building a clear governance framework.

Board and executive ownership and accountability can help by effectively communicating the purpose and importance of a future strategy and allocating sufficient capital resourcing to succeed.

02

Move to perpetual KYC

Financial institutions need to re-imagine the way they conduct KYC. This starts with digitising KYC to improve data quality, enhance compliance, and improve customer experience by automating customer onboarding.

Institutions need more relevant KYC data to obtain a better understanding of customers and their risk profiles, and to develop perpetual KYC by moving away from static customer periodic review models to real-time monitoring with event-driven reviews.

The benefits will include improved customer experience throughout the lifecycle of a customer relationship, combined with an enhanced risk-based approach enabling a more effective use of resources.

03

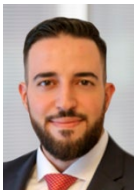
Innovate customer monitoring, starting with complex and intelligence led ML/TF

Financial institutions should strive for a layered approach to monitoring which includes rules-based engines, data analytics platforms, and human intelligence and intuition. The challenge for financial institutions is the need to transform monitoring systems while continuing to operate and deliver services.

A starting point in the path to next generation tools is the optimisation of rules-based engines, based on qualitative and quantitative data. Rules-based systems should be augmented with intelligence-led analytical tools that target complex scenarios, for example, complex money laundering / terrorism financing risk assessments.

Adopting these systems and tools in stages will allow institutions to build toward holistic behavioural monitoring over time. The return on investment will be realised in the reduction of false positive alerts.

The use of machine learning should be explored by targeting specific use cases, and the technology stack should develop holistically in a strategic way. Developing your technology blueprint early will allow you to realise quick wins while working towards the strategic target state.



"Companies are increasing their focus on innovating with data and technology in combatting financial crime and keeping up with new typologies."

Haytham Jaber - Director Financial Crime

CALL TO ACTION

While some of these changes seem a long way in the future, the good news is that financial institutions can start now. We have highlighted 6 calls to action that financial institutions can consider now to better combat financial crime:

04

Fix your data today but don't wait for it to be perfect

Data aggregation can accelerate the implementation of effective financial crime systems. Clean and consistent data is ideal to take efforts to combat financial crime to the next level.

However, the data does not need to be perfect as there are tools that can work with imperfect data. Review current data mining and cleaning practices, and refine the procedures based on previous lessons learned. This approach will allow you to develop data management capabilities and support a generation of better-quality data, without waiting idly for an overhaul solution.

05

Align transformation to a strategic plan and continue to innovate

The process to transform your financial crime compliance program is continuous and should not be locked into a fixed timeframe. In the past, we have been asked when a financial crime compliance program will be 'fixed' - this can be short sighted as the journey to transform takes time.

However, financial institutions should not hide behind the fact that this is a journey. Financial crime transformation needs to demonstrate value through efficiency gains and better prevention and detection in the short term while working towards long-term objectives.

06

Empower financial crime operations

Too often, financial crime operations teams are relegated to the role of being a recipient rather than an integral part of the financial crime ecosystem.

It's time for financial crime operations teams to be connected to the transformation. They hold a wealth of knowledge on the threats facing institutions, which should enable a feedback loop providing insights to inform risk assessments and support rule setting.

However, to play this role effectively, financial crime operations teams need to be in a position to contribute. This means that they need to combine an operations focus with a risk mindset, work with a fit-for-purpose operating model and use process automation to drive efficiency.

"While budgets are tight, we see that many companies continue to invest in strengthening their financial crime capabilities, as there is a clear return on investment"

Ian Nelson - Partner, Head of Financial Services, Head of Regulatory Consulting

HOW KPMG CAN HELP

KPMG's Financial Crime transformation team is at the forefront in expertise and tools to help set you up for success:

- Develop strategic roadmaps based on key pillars and design principles that document the journey from remediation to transformation, that is unique to you and your business.
- Implement our global perpetual KYC solution, developed internally in partnership with Quantexa, to help you transition to enhanced KYC.
- Develop and execute a technology strategy and operating model that supports the utilisation and development of existing and future data.
- Advise on the right tools, technology, strategy, analytics, and data to help you move to innovative customer monitoring.
- Global better practice insights and intelligence to help you shift the mindset towards transformation and innovation.
- Support with optimising and digitising Financial Crime Operations to drive growth and focus on intelligence.
- Enable our client's financial crime transformation strategy, design, and delivery.

The views expressed in this report cover various perspectives on the fight against financial crime. Taken together, they create a valuable combination of insight and expertise. Many of the views expressed in this report may be personal and not necessarily represent those of the organisations the global leaders represent or that of KPMG.

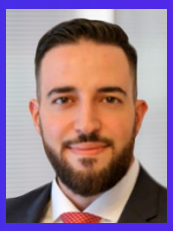
Links to articles: KPMG Australia: Financial Crime, A Paradigm Shift **Click here**

GET IN TOUCH

Ian Nelson
Partner
Head of Financial Services,
Head of Regulatory Consulting
m: + 353 87 7441989
e: ian.nelson@kpmg.ie

Patrick Farrell
Partner
Head of Advisory Markets
m: + 353 87 050 4029
e: patrick.farrell@kpmg.ie

Niamh Lambe
Managing Director
Head of Financial Crime
m: + 353 87 0504388
e: niamh.lambe@kpmg.ie



Haytham Jaber
Director
Financial Crime
m: +353 87 111 6978
e: haytham.jaber@kpmg.ie

Rachel McMahon
Associate Director
Risk Consulting
m: +353 87 111 7961
e: rachel.mcmahon@kpmg.ie

kpmg.ie

Produced by: KPMG's Creative Services. Publication Date: March 2023. (9117)