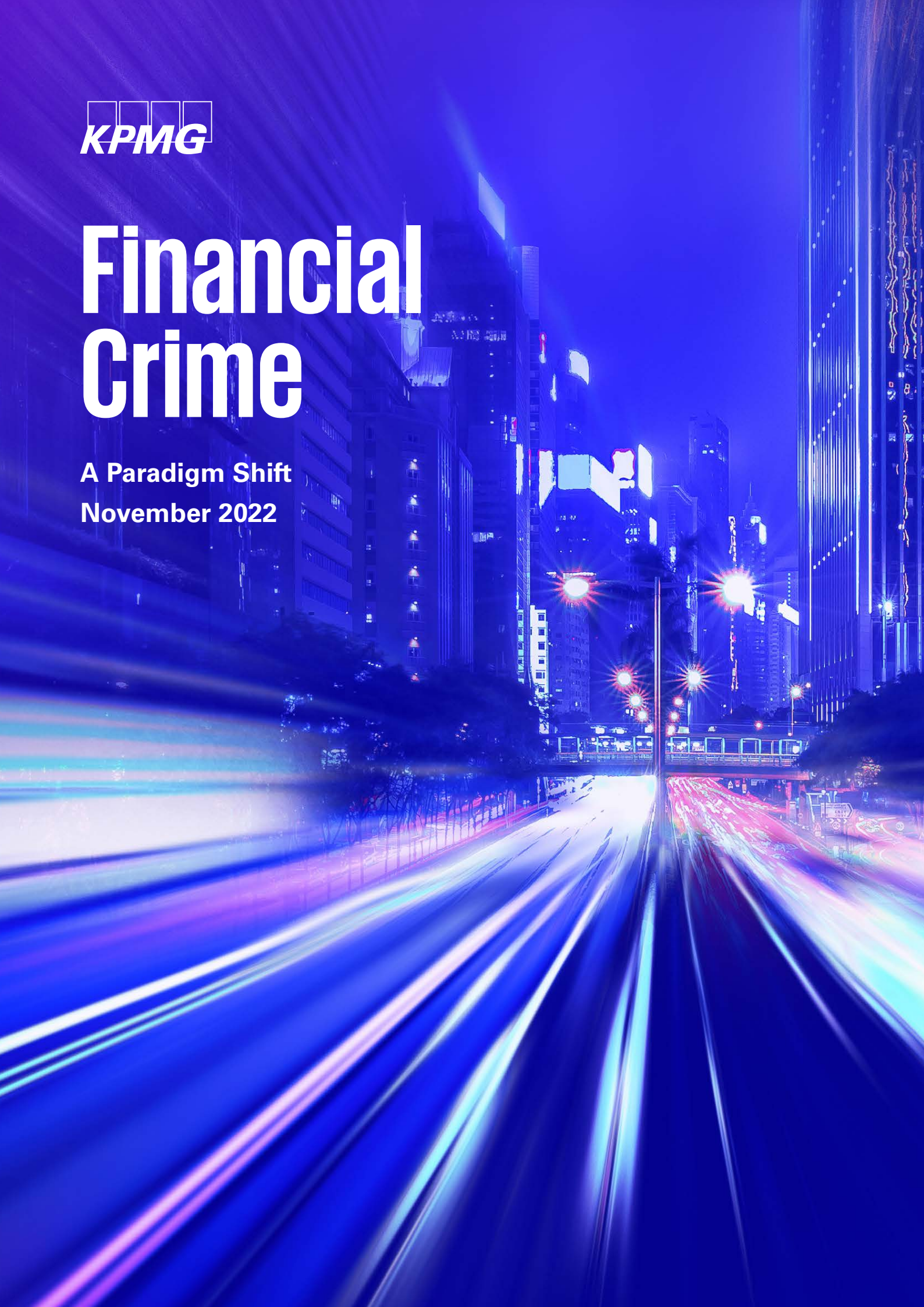


KPMG

Financial Crime

A Paradigm Shift

November 2022

CONTENTS

Section one

Foreword

FOREWORD – SUE BRADFORD

Financial crime has become one of the most significant risks faced by financial institutions and global economies. Almost all criminal activities committed globally are profit driven. Most, if not all, of these involve some form of financial crime, including money laundering.

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.

Whilst fighting financial crime has been a priority for regulators and financial institutions, both are under immense pressure to move away from 'tick-box' compliance by innovating and promoting a culture of compliance to better protect our communities.

This publication, "Financial Crime: a Paradigm Shift", brings together the views of highly experienced and passionate thought leaders from across the globe to understand why the fight against financial crime matters, gauge the current climate, and identify shifts or changes in the future of financial crime required to move forward with purpose. This series of unique articles features leading commentators from industry, government, RegTech, law enforcement, consulting, and academia; each offering unique insights, perspectives and bold predictions about financial crime and the evolving state of play.

Each interview offered inspiring and pragmatic perspectives on how investment, strategy and change can affect meaningful progress in the fight against financial crime. A call for more entities to take initiative in refocussing public-private partnerships and enhance inter-agency cooperation was emphasised as a foundation for transforming the fight against crime.

We explored the ongoing development in technology that enables the movement of funds with increasing efficiency, and the challenges and opportunities these advances pose to financial institutions and regulators in maintaining pace to prevent exploitation.

In discussing the paradigm shift in the fight against financial crime, we have considered the upcoming trends expected to emerge and leveraged our expertise locally and globally across the market as a leader in financial crime transformation.

This publication provides a series of expert perspectives exploring how financial institutions can be at the forefront in taking action to better safeguard communities and disrupt or prevent financial crime more effectively. We are encouraged that the sentiments and perspectives presented here are echoed throughout the broader network of professionals and industries, and will materialise as we continue to strive for effective advancements in financial crime prevention over years to come. We have also explored how financial institutions can be at the forefront in taking action to safeguard the community and help disrupt financial crime more effectively. I am encouraged that our clients can collectively aspire to deliver on these visions of the future, together working boldly to tackle financial crime that promises tangible economic and social benefits.

Sue Bradford,
Partner KPMG Forensic

FOREWORD – TIMOTHY GOODRICK

As the criminal threat becomes more complex in Australia, we need to leverage new and innovative methods to combat financial crime. The way forward will be challenging, requiring diverse perspectives and an appetite to transform.

When we started interviewing global thought leaders about the paradigm shift in the fight against financial crime, we didn't know what to expect. While I had known some commentators for years, others I was meeting for the first time. Yet in all interviews, one word came to mind – inspirational.

Today, we know only too well the cost of financial crime to people, profits, and the planet. Financial crime affects our communities, businesses, and the Australian economy. The criminal threat we are facing today is more complex and challenging than it has ever been. This is why we need a paradigm shift in the way we combat financial crime.

We interviewed leaders from law enforcement, academia, international bodies, the financial sector, and consulting. Each leader walked a different path to get to the top of their profession, but they all share the same objective – to combat criminals and terrorists by hitting them where it hurts: their money.

One thing we know for certain is that criminals adapt – organised crime groups find new ways to launder money, terrorist organisations find new ways to raise and use funds, and people find new ways to evade sanctions. I recall around 15 years ago speaking with a leading figure in law enforcement in Australia who compared it to an arms race – as soon as we put controls in place to prevent or detect financial crime, criminals are already searching for ways to get around it. This rings as true today as it did then.

The Australian financial crime community must adapt and innovate to ensure that the tools we have are effective. We need to use these changes to our advantage, starting with better use of data and technology. This is the future in the fight against financial crime. In every interview, we heard that data and technology will underpin how we detect crime, and how we manage financial crime programs of the future.

A future-looking financial crime program is one that is strategically designed, integrated with business operations, cost-effective, attentive to customer experience, and agile in responding to new and emerging threats. As the level of regulatory scrutiny in combatting financial crime increases, regulated businesses will need to frequently examine whether what they are doing is effective.

While we are facing significant challenges in the fight against financial crime, we also have a significant opportunity. We need to think strategically by laying the foundations for an effective financial crime program of the future, while also acting tactically by targeting the financial crime threats that we are facing today.

And we need to continue working together as a community. There was agreement among the leaders interviewed that public-private partnerships will play a key role in the paradigm shift. The starting point of an effective public-private partnership is trust and a common purpose. Based on these interviews, I know we are in good hands.

Having listened to these global leaders, I am confident that we have the collective will and capability as a global community to sustain the paradigm shift in the fight against financial crime.

Timothy Goodrick,
Director KPMG Forensic

Section two

KPMG Point of view

FIGHTING FINANCIAL CRIME

The Paradigm Shift

Global financial crime experts are foreseeing a fundamental shift in how organisations approach compliance over the next decade, as the criminal threat becomes more challenging and complex.

Based on our interviews with 16 global thought leaders, we have identified 6 major trends that we anticipate will shift the paradigm of disrupting financial crime compliance over the next 5 – 10 years:

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.

Call to Action

The coming paradigm shift will require large-scale transformation and commitment across the industry. This evolution must begin now. Our research has identified 6 steps that organisations can take to better combat financial crime:

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.

POINT OF VIEW

Financial institutions in Australia are facing increasing community and regulatory pressure to implement effective systems that combat financial crime and encourage meaningful positive impact, rather than just 'tick the box' compliance.

The cost of financial crime on communities, economies, and the planet, has been felt around the globe. Financial crime is not a victimless crime. Each year, money that has been stolen, laundered, or otherwise illegally obtained enables activity that harms people and communities, such as modern slavery, drug and wildlife trafficking, and corruption. Proceeds from serious and organised crime need to be laundered, that typically occurs through the financial system and results in significant costs to society.

A recent report by the Australian Institute of Criminology estimated the cost of serious and organised crime in Australia during 2020 – 21 at $60.1 billion . These costs are borne by the Australian taxpayer, law enforcement agencies, and financial institutions. For regulated entities, the reputational, financial, and legal consequences of financial crime can be severe.

This report explores trends, themes, and bold predictions that professionals around the globe expect will occur in financial crime and prevention over the next 10 years. We interviewed 16 thought leaders from industry, government, RegTech, law enforcement, consulting, and academia to discuss where the journey in combatting financial crime will lead, and the paradigm shift we will need to get there.

At KPMG, we believe that how you grow matters, and that economic growth shouldn't come at all costs. We believe that you can push forward without sending the world backwards. Our growth should better us all, beyond today. Combatting financial crime is a key component to our environmental, social, and governance (ESG) lens at KPMG.

Combatting financial crime matters

Financial crime is a global and large-scale problem that has a widespread and devastating impact. This is why combatting financial crime matters.

Among the leaders we interviewed, a single constant emerged – combatting financial crime is much more than a job, it's a passion. The driving force that gets these leaders out of bed each morning is the ability to contribute in the fight to protect society, our communities, and our planet.

All profit-motivated crime requires money to be laundered through financial institutions. This facilitates further crime by allowing criminals to enjoy their ill-gotten profits and re-invest in additional criminal activity such as modern slavery, drug trafficking, environmental crime, tax evasion, bribery and corruption, and fraud.

Financial institutions are at the forefront of the global effort to combat financial crime.

The criminal threat environment is increasingly complex

The criminal threat environment in Australia has become increasingly sophisticated and complex. Criminals adapt to avoid the controls we have in place today which leads to displacement. As we block off one avenue to funnel illicit funds, criminals look for other ways and techniques to successfully launder money and avoid detection.

We are witnessing a convergence of cyber-crime and financial crime as technology enables new ways to launder illicit funds. This, combined with the increased role of professional money launderers that are more globally connected than ever before, has resulted in new and emerging threats. Physical cash is reducing which will increase the vulnerability of other monetary forms such as virtual assets.

Governments and financial institutions need to understand the evolving criminal threat environment to ensure that their financial crime compliance systems are risk-based and effective.

The financial crime paradigm shift will be an evolution

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

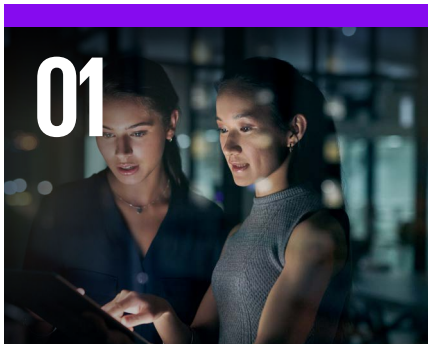
We see this as more of an evolution rather than a revolution as advancements will take place over time, and at different speeds depending on the organisation.

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

1. Estimating the costs of serious and organised crime in Australia, 2020–21 https://www.aic.gov.au/publications/sr/sr38

POINT OF VIEW

Our view on what the shifts 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 it is 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.

POINT OF VIEW

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 data-driven, 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 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

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 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.

CALL TO ACTION

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.

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 a 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 chorus 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.

Section three

Articles

JOHN MOSS

DEPUTY CEO INTELLIGENCE
AUSTRAC

As the Deputy CEO leading the Intelligence Division, John has senior leadership for Australia's Financial Intelligence Unit (FIU) including intelligence operations, partnerships and capability programs, international activity, Fintel Alliance, taskforces and specialist cyber capabilities.

PETER SOROS

DEPUTY CEO REGULATION, EDUCATION AND POLICY, AUSTRAC

Peter commenced at AUSTRAC in June 2018. He is responsible for the regulatory and compliance operations of AUSTRAC. He also has responsibility for AUSTRAC's legal, policy and communication functions. A key element of his work is overseeing AUSTRAC's enforcement activities.

“

The explosion of public-private partnerships and working together to analyse different sources of information will be the key to future progress in combatting financial crime. If we pull together, we can achieve more.

JOHN MOSS

DEPUTY CEO INTELLIGENCE – AUSTRAC

[John]: Having spent my career investigating serious organised crime and helping to protect Australia's national security, I was surprised by how nuanced and complex the financial crime challenge was when I joined AUSTRAC. I see an untapped utility of financial information across law enforcement, national security, and industry that can be used to help combat criminal activity – 6 years later, this challenge is what holds me here.

[Peter]: After spending my career in public service and having a helicopter overview of the national security architecture, I found that not a lot of national security spaces engage or rely so heavily on the private sector as much as they do in AML/CTF. This is what attracted me to this space. Since joining AUSTRAC, I have been pleasantly surprised and fascinated by the genuine commitment to partnerships and collaborating on issues.

Money laundering trends

There are three enablers helping to facilitate organised crime, particularly financial crime:

1. Increased online activity, either via traditional online ransomware or cyber as an enabler – almost everything is touched by some form of online activity.
2. Increased integration between jurisdictions – it has become common to have a victim, perpetrator, and profit in separate jurisdictions.
3. Scale and volume of data is immense, and criminals are using it now more than ever to hide both legitimate and illegitimate activity.

Given these new ML/TF risk dynamics government agencies and reporting entities need to evolve their capabilities and systems to remain able to detect and deter. For example, when a bank comes to us with a 4-year rigid uplift program, we can see that there will be challenges to remain current. However, banks are realising that they need a program that can mature and evolve over time to keep up with criminal trends.

Public-Private Partnerships

Increased public-private partnerships where we are working together to analyse different sources of information is key to future progress in combatting financial crime. If we pull together, we can achieve more at a greater scale. A driver behind this will be the private sector's willingness to take the initiative as the early adopters of technology, coupled with investment. Part of the equation for the future will be facilitating different collaboration models and using the Fintel Alliance to obtain a richer industry picture. The real question to really enhance our efforts to combat financial crime will be whether public-private partnerships will collaborate globally.

Data and Technology

Leveraging technology and advanced data analysis capabilities is another key aspect in the fight of fighting financial crime in the future. We have buckets of data that may be unstructured and not easily searchable in its current form, and I predict that this will be the case for another 3 or 4 years.

Analysis of big data will be critical as we develop intelligence from multiple sources and increasingly sophisticated systems. We will see tools that lawfully and appropriately search billions of records across multiple datasets in real-time. There are a whole range of tools emerging that allow that, and how we deal with information is on the cusp of change.

Financial crime is detection and response; we have a thin layer of sharing information through partner agencies. We are privileged in the data we can collect and track: it is better than most institutions globally. Banks also have huge amounts of data which adds weight to the need for collaboration.

Resourcing and Culture

There is an uplift occurring across all regulated sectors with organisations now taking a sensible and pragmatic approach to resourcing and skilling. That is partly a consequence of AUSTRAC enforcement action, and we make no apologies for that. Over many years there has been an underinvestment in technology and skilled resources to address the AML/CTF evolving challenges. The findings of the recent Royal Commission[2] highlighting failings in risk and compliance management has also driven the demand for skilled resources.

Another key aspect will be organisational culture. Developing a strong risk culture is difficult for everybody. But when you come out the other side, the tangible impact and benefit to the community is the greatest motivator. No amount of system upgrade or staff hired will be as successful unless you have the right risk culture.

Future Considerations

We want to ensure that all industry sectors susceptible to financial crime risk are involved in the discussion on Australia's national strategy to combat financial crime. From our perspective, the more inputs we receive the better, as more sectors are potentially at risk of exploitation.

The global framework set by the Financial Action Task Force (FATF) will need to keep pace with industry developments and increased risk environment. In the medium term, customers might not have bank accounts and instead use digital wallets or a platform not yet available to customers but might be using digital wallets for payment. One challenge will be the introduction of cryptocurrencies and virtual payments in large-scale money laundering, because of the clandestine nature and fluctuation of those assets. As they stabilise and become more mainstream, there will be capabilities required to respond to those new threats.

A last point to make is around the value of international cooperation. We have been focused on the countries that we trust to speak the same risk language. We are also continuing to work closely with our offshore counterparts in other financial centres, and are integrating moree with other parts of the government. We want to ensure that the right strategic partners are working with AUSTRAC, to ensure we bring together a range of capabilities and functions, and work holistically to combat money laundering and terrorism financing across borders.

2. Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, report delivered on 1 February 2019, https://financialservices.royalcommission.gov.au

> "Banks are realising that they need a program that can mature and evolve over time to keep up with criminal trends.

PETER SOROS

DEPUTY CEO REGULATION, EDUCATION AND POLICY – AUSTRAC

Alexon is the Chief Product Officer at Quantexa and has more than 20 years' experience helping global organisations meet their AML regulation requirements. By creating a new approach to AML monitoring, Alexon works closely with customers to build, deploy, and optimise AML systems across numerous areas, including trade and correspondent banking, to reduce cost and risk. He transforms the way businesses work with data to improve compliance, investigation, and KYC processes to successfully detect criminal activity, such as money laundering, human trafficking, and terrorist financing.

I fell in love with anti-money laundering partly because of the analytical challenge, but more so because preventing terrorist attacks and finding human traffickers has a positive impact in the market. There is a calling when you see how organised crime erodes the fabric of society, and the social consequences that come with it.

As one of the founders of Quantexa, I am fortunate to continue our mission of changing the approach to disrupting and detecting financial crime. I started my journey with the Financial Intelligence Unit of a global bank, building an alert management and customer due diligence utility and a ground-up software which ingested and resolved billions of rows of data. We then built a solution which resolved all parties to a single transaction and pioneered contextual monitoring. The key to success was enriched data, so we developed a master data management program that could detect criminals and generate new business for the bank.

I believe data is key to future progress. Every customer has a digital footprint, and the ability to know everything about your customer or their business is essential to understanding who that customer is, their touchpoints within the bank – and to detecting actual crime.

In the next ten years, I hope to see a convergence of KYC, transaction monitoring and sanctions screening into a single KYC system. If each system is designed to determine customer risk, you can only obtain a deeper understanding of your customer's risk by looking at it holistically.

KYC will look completely different in 10 years' time; there will not be an army of people constantly updating records but systems performing KYC continuously (no more calendar reviews, trigger based KYC will be the standard) and seamlessly integrated with Risk scoring and monitoring. We will also see movement towards viewing the counterparty as fundamental. If we know that financial crime is highly collusive, where are the connections between entities?

ALEXON BELL

CHIEF PRODUCT OFFICER
QUANTEXA

With an entity enriched network, we will be able to review suspicious activity reports and determine which contain meaningful data. We have already started to see the power of enriched data and segmentation models providing a feedback loop to AI and detection systems. As we continue to enrich our data, we will have moved into a phase where AI delivers value to organisations. With the right support from regulators, new technology can be deployed to detect undiscovered criminal activity. The high rate of false positives will be minimal due to the utilisation of such technology and enriched data.

Information sharing will be pivotal for the future. We know that criminals typically bank with at least six institutions, however you only see a small portion of that activity. A cooperative framework that encourages sharing between cohort banks will help feed a continuous investigate and detect cycle. Technology can support this now, but it will probably take 10 years, to get social and legal acceptance and we will have the ability to join datasets together, allowing you to find entire networks of criminals that your customers have transacted with. No one knew about them beforehand, but now you do.

Regulators must continue to embrace innovation in data and technology, by hiring technologists who can fully understand the effects of AI and its ability to help banks comply with regulation. Regulators understanding the impact of technological innovation is key to allow information sharing from the top down.

While the global cost of compliance continues to increase, it will shift from people to technology. Currently 75% of a budget is spent on employees and 25% on technology and software licenses, however I predict this will switch in the near future. Public-private data sharing is not free, and innovation should not stop. You must be able to share and collaborate.

Data is useless without the technological infrastructure to support, analyse and disseminate information. In the next 10 years, there will be a devolution or 'sun setting' of platforms with archaic systems which cannot work in a modern era. Investment in technologies with AI that can support a transition into the future will be vital but requires the right mindset and vision of where you need to be. Banks will be key to disrupting the current crime ecosystem; they are the ones who will say "I've had enough, there must be a better way".

All opinions expressed here are Alexon's own.

"

Everything to do with AML is about data, but the data is useless without the technology to use it.

ALEXON BELL

CHIEF PRODUCT OFFICER
QUANTEXA

Jennifer is HSBC's Group Head of Financial Crime and Money Laundering Reporting Officer. She previously served as the director of the Financial Crimes Enforcement Network (FinCEN) for the United States Department of Treasury. Jennifer also spent 15 years as a prosecutor in the Department of Justice, focussing on combatting criminal financial schemes, international organised crime groups, and professional money launderers.

From an early age, I was inspired to enter a career combatting crime by my grandfather, a police officer who attended the FBI's National Law Enforcement Academy and ultimately became a police chief. I majored in International Affairs and attended law school, intending to enter the intelligence profession. Instead, I became a prosecutor at the US Department of Justice, focussing on Russian organised crime.

The more I looked at the extent of the problem, the more convinced I became of the importance of the US Government's role in combatting illicit finance. This put me on the path to fight financial crime and led me to serve as the Director of the Financial Crimes Enforcement Network (FinCEN).

I am motivated by making significant impact for good. I have spent my career preventing illicit money flowing through the financial system, because if you do that, you remove the reward and motivation behind organised crime syndicates. Today, a focus on effectiveness in anti-money laundering and counter-terrorist financing (AML/CTF) programmes and the power of innovative technology are leading us to a paradigm shift in the way we tackle illicit finance.

Today's Risk Landscape

The economic impacts of the pandemic have caused large corporate, accounting, and trade financing fraud. We have seen examples of fraudsters taking advantage of government assistance programs procuring scarce goods like masks and oxygen.

As we pursue a net zero agenda, minerals and materials required for climate solutions will become difficult to source, providing opportunities for criminals to exploit the resources that are vital for our future.

Rapid innovation is occurring as FinTechs, traditional banks, neobanks, and digital currency providers fight to provide more efficient and effective solutions. The challenge for regulations is to keep up with this pace of change and address any opportunities for illicit finance that it creates.

JENNIFER SHASKY CALVERY

GROUP HEAD OF FINANCIAL CRIME, HSBC

“Your data does not have to be perfect to solve the problem of financial crime.

JENNIFER SHASKY CALVERY
GROUP HEAD OF FINANCIAL CRIME, HSBC

Regulatory Environment

As new players enter the payments space, regulators need to ensure an even playing field by regulating the same activity in the same way. Any regulatory gaps or uneven application of standards will impact transparency and disadvantage detection and prevention.

As a result of both FATF's, and the industry's work on effectiveness, regulators and policy makers in the US, UK and Singapore are now focused on effectiveness more than ever, including whether resources are being targeted at the most pertinent areas of risk in order to detect and deter financial crime. Regulators can encourage firms to focus on making their AML/CTF programmes more effective and be less prescriptive about how we get there. It will take collective courage.

Proactive Intelligence

As employees know the organisation better than anyone else, we encourage our teams to assume the position of a criminal and ask – if I were going to launder money through my bank, how would I do it?

Firms are moving toward bespoke thematic intelligence or large-scale automated processes. I would encourage any firm, no matter their size, to have a financial intelligence unit conducting bespoke thematic intelligence assessments.

The fusion of policies, controls and technology covering fraud and financial crime will ensure your data, tools and processes are as integrated as possible. When you look at the framework design holistically, you can start to bring together opportunities for proactive intelligence.

The Power of Typologies

The first step to sourcing better intelligence is creating a typology library. Find out what typologies or red flag indicators AUSTRAC provides, identify those that apply to your institution's customer base and products, and assess what data your bank holds. Then you can investigate how typologies manifest in your bank, the data required to identify them, and how to capture that data.

There is a limited number of ways to move and launder money. Once you have a clear view of what they are and how you detect them, suddenly you have coverage across all your crime types.

Harnessing Data

Your data does not have to be perfect to solve the problem of financial crime. Analytics can help to make sense of it, and humans ultimately look at the results. Just get it as good as it can be, whether it is centralised or de-centralised, as there is technology for both.

You need to be able to look at your data in the countries in which you operate, process it at speed, and have resources to apply analytics. Staff should be trained to understand your data, and be able to explain the analysis and outcomes in plain English to a regulator.

KYC/CDD

When onboarding new customers, you are doing two things, 1) determining whether the customer fits within risk appetite; and 2) collecting basic data that will allow you to understand your customer's behaviour and see if what they say is true, and identify any changes over time.

If the standard of your back-book customers is not where it needs to be, there is nothing you can do but remediate. To do that successfully, you need to have a defined target end state with measurable criteria. That takes time to define, but do the hard work, because when you do it right, it pays off.

The Importance of Culture

Ask yourself how comfortable you are with the way your bank is detecting criminal activity.

The right culture is integral, starting with the CEO and Chair of the Board at the top, and sown into incentives throughout the bank. Regulators want to see that you understand your risk, are comfortable managing it, and are not the type of bank that accepts criminals because you need the customers and are looking for profits. If you have that culture, you have a problem.

All opinions expressed here are Jennifer's own.

ROBERT DEAN

HEAD OF FINANCIAL CRIME TECHNOLOGY
KPMG UK

Robert is the Head of Financial Crime Technology at KPMG in the UK. He is a leading authority in the field of machine learning and artificial intelligence in financial crime control systems, speaking at a broad range of industry events, global conferences, and participating in panel debates alongside financial services regulators, industry SMEs and academics. Robert most recently led the development of KPMG in the UK's proprietary algorithmic classification platform for expediting the operational and case management aspects of many different alert review processes, including both sanctions and transaction monitoring alert reviews.

Anti-money laundering is fundamentally the right thing to do – it prevents significant societal harm that criminal exploitation and financial crime generates. When I initially became involved in anti-money laundering, the motivation was problem solving the functionality of data and technology. There were many situations where banks had 10 years' worth of data, but the reports were not contributing to the determination of whether compliance and proper due diligence had been undertaken. I became hooked on improving and advancing the tech to better process and interpret data.

10 years from now, I believe we will have good data and stronger technology. Good data is comprehensive, contemporaneous, and accurate in terms of depicting customer activity and transactions. The improved quality of data will make it fit for purpose and better able to primarily support the prevention of illicit finances, and subsequently the compliance practices of banks.

There also needs to be a shift away from the compliance and tick-box attitude of organisations to AML. When these organisations have access to both sides of the transaction – the customer and the subsequent activity – there is an opportunity to detect what is occurring. Improved transparency over payment processing as a result of the ISO20022 migration also means this data can be leveraged as a preventative control. Organisations need to critically review their current approaches and infrastructure, reflect on lessons learned from earlier practices, and engage a preventative approach.

I believe Reg-Tech type organisations will innovate because it is in their nature. But there needs to be an ambition from regulators globally to collaborate and agree on innovation and new standards. There cannot be disparity in expectations and standards among regulators or inter-governmental organisations or you will not be able to operate.

A year ago, I would've labelled the US as the most conservative example of regulation in the space – but now they are leading innovation. The US is changing and evolving and willing to accept more advanced technologies. It would be unrealistic to suggest a mandate for artificial intelligence and machine learning, but we need to move beyond being complacent with old technology and practices just because they are familiar.

Although organisations are right to be concerned with the economics of their transaction monitoring practices, they also need to question if their financial crime prevention models are achieving their purpose. To ensure financial crime prevention models are functioning optimally in organisations, many will need to move away from their current siloed approaches for transaction monitoring and towards enhanced data-sharing.

The biggest opportunity for change moving forward is transaction monitoring. To respond to the cross-border and networked nature of payments, transaction monitoring needs to become more centralised to establish comprehensive visibility.

It may be necessary to consider the role of a global entity to collate data and undertake transaction monitoring and set new standards in what degree of risk in payment patterns is acceptable.

I believe transaction monitoring in the future is attuned to the risks and anomalies rather than burdened with mass data mining. Monitoring systems can only advance with quality data, so improved data-sharing efforts and practices will be necessary to support this. It is less about the customers that you do generate alerts on in the monitoring process, and more about the customers who continuously evade having alerts raised on their activities - the latter is far more dangerous than any of the customers you do detect.

When people consider technological advancement and improving the data, it often becomes a cost-benefit analysis. The reality is the cost of compliance to banks is passed down to its customers. This leads to a vicious cycle of banks offering competitive prices to keep customers, at the expense of thorough and effective preventative controls which makes those entities targets for exploitation by criminals and fraudsters. I do not believe the current costing is sustainable, but it can only change with concerted effort from banks and regulators focussing on the strategic goal of more economic and effective means of achieving their objectives.

> "I think most of the money is spent today ticking the boxes and meeting the expectations of the regulator, rather than actually generating useful output.

ROBERT DEAN

HEAD OF FINANCIAL CRIME TECHNOLOGY KPMG UK

PAUL JEVTOVIC

CHIEF FINANCIAL CRIME RISK & GROUP MONEY LAUNDERING REPORTING OFFICER, NATIONAL AUSTRALIA BANK

Paul is currently the Chief Financial Crime Risk & Group MLRO with NAB and the former Regional MLRO & Head of Financial Crime, Asia Pacific for HSBC. Prior to working in the banking sector, Paul held multiple senior positions across Australian law enforcement agencies including AUSTRAC, ACC (now ACIC), OPI and AFP.

As the CEO of AUSTRAC, Paul oversaw the investigation of AML misconduct by TABCORP and Commonwealth Bank, and led the establishment of the FINTEL Alliance among regulators, banks and other entities in the Australian AML community.

Paul was awarded the APM for his extensive career in state and federal policing, and the OAM for his outstanding commitment to AML enforcement and securitisation of the Australian financial sector against criminal compromise.

Throughout my upbringing it was instilled in me that we are fortunate to be Australian and the need to give back to make Australia a better place.

I started in the Australian Federal Police almost 40 years ago and have since worked nationally and internationally. During my 30 years in policing, I witnessed how instrumental financial flows and assets were to the continued perpetration of harmful crime. I believe that preventing these illicit finances from being laundered in our legitimate sectors protects the integrity of our domestic markets and decreases the lucrativeness of those illegal operations.

Accelerate the evolution of financial crime prevention

We must understand that criminals are lawless, moralless, jurisdictionless and boundless. They are embracing technology at a faster pace and have the capability to do crime at scale, at speed and can attack all around the world from one location.

To combat this, I hope to see an acceleration in the evolution of financial crime prevention. Technology enabled crime has already been well and truly embraced by criminals and they will only become more sophisticated in how they maximise its harm on our communities. In turn, to get ahead of criminals, we too must invest in solutions for the future in a sustainable and consistent manner.

“

We need to evolve to continue to harden the nation against financial crime.

PAUL JEVTOVIC

CHIEF FINANCIAL CRIME RISK & GROUP MONEY LAUNDERING REPORTING OFFICER, NATIONAL AUSTRALIA BANK

Evolving our use of technology

Technology and data are at the core of how we evolve in the fight against financial crime. We need to embrace technology at pace to get ahead of the criminals, while at the same continuing to invest in our people and their capabilities to maxmise the opportunities that data and technology present.

Organisations that are doing well are using technology to understand the customer holistically. Understanding who a customer is, what they do and with whom supports organisations with undertaking close to real-time risk management as opposed to when performing transaction analysis alone.

A critical component to holistically understand a customer is to centralise customer data, and to improve the accessibility and integrity of the data. Maximising the use of data allows us to be proactive and preventative. While data analytics in financial crime has been used for 10 years, there are opportunities to maximise its use and to embrace cloud-based machine learning.

To improve financial crime compliance and technology, RegTech vendors must also evolve their solutions to accept the less than perfect data that organisations hold. Good vendors are already designing cloud-based platforms that address this.

As we continue to adopt technology it must be noted that vendors will need to be able to communicate with less technologically savvy clients, including possessing the ability to explain their system in a court environment; smart vendors can do this.

Public-private collaboration is required

There is a need to think holistically as financial crime is a collective problem of banks, regulators, and the community. We need to evolve to continue to harden the nation against financial crime.

Banks should be able to collaborate more and communicate in real-time on risks being confronted. This may require a change in privacy laws as it is time to evolve the concept of privacy to support a unified approach in protecting the community.

Private Public Partnerships (PPPs) should be a focus and going forward we should use them to maximise both bank and law enforcement data. For PPPs to be effective there must be a genuine partnership with two-way information flows.

We also have to consider the financial system as a whole. One bank’s success should not be another’s misery and we want customers to stay within our financial infrastructure. Financial crime should not be survival of the fittest, or which bank has the most to spend to the detriment of smaller bank and PPPs should support this.

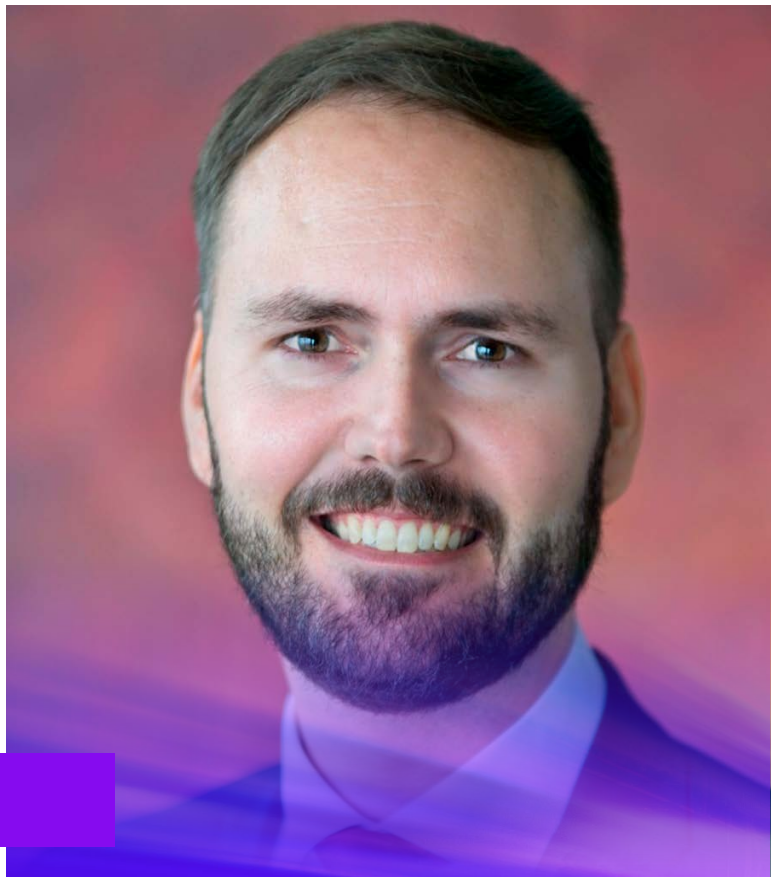
Further, I see it as important to bring together experts to address financial crime. There is an important role of academia, think tanks and RegTech. There is also an opportunity to bring the public and customers into the solution.

Importance of culture

We can have all the data and technology in the world, however without the right organisational culture, we are left wanting.

Everyone in the organisation needs to understand the role they play and embrace it. Financial crime threat management cannot be left to pockets of individuals.

Organisations need to continue encouraging people to speak up and do the right thing. Going forward, good and proactive behaviour needs to be encouraged, recognised and incentivised.



CHRIS KAHTS

GROUP HEAD OF FINANCIAL CRIME
MACQUARIE GROUP

In 2020, Chris joined the Macquarie Group as Group Head of Financial Crime. Previously, Chris was Head of Financial Crime at Barclays International.

Financial institutions are the fundamental enablers to society. We cannot do anything without some form of account with a financial institution; they are pivotal to everything we do and therefore pivotal to combatting financial crime.

Banks are at the heart of everything and often have the biggest scale of impact in combatting crime when systems, controls, and processes are geared towards disrupting the harm that financial crime has to society.

I happened upon the discipline of managing financial crime risk in banking several years ago and have remained in financial crime risk management for almost a decade. It is an incredible job when not only do you get to play a role in stopping bad things happening in society, but you get to do it as your day job.

It is hard to say that there will not be a change in threats and vulnerabilities in 5 to 10 years. Using the last decade as a proxy for what might come in 10 years, we will most likely see substantial changes in the ways in which the financial system is abused.

I think that general innovation will speed up. There is an exponential curve of creativity as communities are enabled and empowered with information and technology. The world of finance, in whatever shape it takes in the future, will transform as the pace of change continues to increase. Our challenges will continue to take new forms, creating a need for continued investment to counter bad actors.

Going back 15 to 20 years, the industry buzzword was around Enterprise Resource Planning (ERP) and how it would transform an organisation as a one stop solution. ERP solutions delivered because there was convergence across many different aspects of running an organisation. I hope that this will happen to financial crime risk management in the future – we need convergence across silos which remain prevalent today. The reality is that combatting financial crime does not rest on a single control or technology solution, a network of controls operates at every point in time to detect and prevent financial crime.

Is the return on risk proportionate to the level of cost?

In the short-term, my answer would be no, but in the long-term the answer must be yes. Friction between cost and obligation drives innovation which ultimately leads to reduced cost.

A sea change has occurred in the last 10 years, and the exploitation of the finance industry has, unfortunately, equally benefited from such innovation.

Will the traditional KYC refresh cycle change in 5 to 10 years' time?

I think the answer changes based on the organisation; domestic firms will, for example, be able to jump on backlogs easier than an organisation with international presence. This distracts from a financial institution's ability to build something once that benefits the firm globally. In the long-term, I think we will see increasing regulatory convergence which will allow firms to create greater scale in internal mechanisms that run component parts of a program such as KYC refresh. Furthermore, as information is more readily available in the public domain, we will likely see a steady move away from concepts of refresh cycles and moreover toward perpetual or exclusively trigger based refresh.

Technology and Data:

Everything we do invariably comes down to technology and data. Organisations often do not use data (both internal and external) to full effect, although industry at large is beginning to exploit the value of data more. The next big thing in industry is likely to be focused on convergence of technologies across components of a financial crime programme. Institutions need to understand their entire program, what they want to achieve and how far they want to go to make sensible and justifiable investments.

In the last 5 to 10 years, public-private partnerships and policy reform have started appearing. Intergovernmental engagement has also increased, which starts to move regulatory expectations towards a common destination.

The speed at which technological innovation progresses in financial institutions will at the end of the day have the greatest impact in combatting criminals. It is about who gets there first – us or the criminals.

All opinions expressed here are Chris' own.

> "The speed at which technological innovation progresses in financial institutions will at the end of the day have the greatest impact in combatting criminals.

CHRIS KAHTS

GROUP HEAD OF FINANCIAL CRIME
MACQUARIE GROUP

TOM KEATINGE

DIRECTOR OF THE CENTRE FOR FINANCIAL CRIME AND SECURITY STUDIES,
ROYAL UNITED SERVICES INSTITUTE

Tom Keatinge is the Director of the Centre for Financial Crime and Security Studies (CFCS) at RUSI, where his research focuses on matters at the intersection of finance and security, including the use of finance as a tool of intelligence and disruption. He has a Master's in Intelligence and International Security from King's College London, where his research focused on the effectiveness of the global counterterror finance regime. Prior to joining RUSI in 2014, he was an investment banker for 20 years at J.P. Morgan.

Tom Keatinge has contributed to a variety of publications and media outlets; has given evidence to parliamentary hearings and spoken at a range of high level forums.

During my 20 years as an investment banker, I took a sabbatical year to study, during which I discovered the magnitude and effects of terrorism financing and money laundering. At that time (2012), awareness among banks of the role they played in facilitating illicit finances that predicate and motivate the incidence of serious and harmful criminal activity, including organised crime and human trafficking, was rare; and efforts to address this role were even rarer.

The investigation of financial crime can be powerful in disrupting such criminal activity. A good example is where financial activity has provided intelligence to disrupt wildlife trafficking and facilitated the arrest of a wanted criminal. Banks and other financial services have the capability to interrogate their data and support the investigation of those crimes. I believe the insights to be gained from financial institutions adds valuable dimensions to fighting financial crime and can significantly improve prevention and earlier detection.

Understanding our current challenges

The evolving nature of money and financial environments is an ongoing challenge. For example, e-currency is challenging because it facilitates cross border flows in a way not anticipated by existing regulation. It is a difficult phenomenon to control and monitor. As traditional banking tightens restrictions, we can see an uptake in its use and abuse in financial crime. Rules and regulations struggle to keep pace. The rise in cryptocurrencies presents a further development challenge for regulators and law enforcement.

Our inability to keep up with the evolving threat environment is an indication of an even bigger concern: our archaic system. I am unimpressed sometimes that new policies appear to be just a new coat of varnish on an old table. It might seem to address the issue, but it does not fix the cracks or underlying vulnerabilities.

“The biggest threat is the failure of the current system’s ability to keep up with new realities.

TOM KEATINGE

DIRECTOR OF THE CENTRE FOR FINANCIAL CRIME AND SECURITY STUDIES
ROYAL UNITED SERVICES INSTITUTE

The current procedures undertaken to comply with AML policies are not optimal. Suspicious Transaction Reports (STRs) must be generated by banks, expending their finite resources for a limited return. I hypothesise that the percentage of valuable STRs generated today has decreased from previous years. Thousands of these STRs are submitted to the regulator/FIU to again expend their limited resources on leads provided by banks that have been generated with imperfect information and are thus unlikely to be of any value.

When I hear conversations about the challenging cost of compliance, I am concerned AML has lost its way. It is reasonable for banks to be conscious of the cost-benefit analysis of this process. By any reasonable measure, the current reporting process is a poor investment for banks and FIUs alike. Banks are spending money on procedures such as STR filing – first and foremost – to keep the regulators happy, rather than investing in systems and procedures that secure the financial system from criminal exploitation. I would like to see both private and public entities consider more closely how their spending can be optimised and achieve real impact and anti-financial crime outcomes.

Enhancing our current approach

A shift towards a more effective eco-system will be driven by two key elements: partnerships and technology. These two features should function symbiotically to achieve the impact and outcome all – from both public and private sectors – should be striving to achieve.

Another important consideration, needed to unlock the impact of these innovations, is for the relationship between regulators and financial institutions to be redefined. I like to describe it this way: you don’t treat a child the same way when they are 12 as you do when they are 22. Relationships change and adapt to new circumstances. This is the same situation for financial crime prevention. There is no doubt that 10 years ago, banks needed strong parenting. Failings were everywhere, systems and procedures were poor or absent entirely. Today, from a compliance perspective, many banks are unrecognisable from their state a decade ago. Regulators should thus adapt the way they engage with financial institutions accordingly, allowing them to develop financial crime responses that reflect their business and experience. Put simply, regulators must embrace the risk-based approach and accept that an effective system will not be a zero risk system.

Furthermore, I am concerned that public-private partnerships increasingly appear as a guise for the public sector to outsource activities to the private sector, rather than investing in their own capabilities. I would like to see the partnerships that have sprung up in many jurisdictions being modernised to embrace modern technology and return to the collaborative spirit that spawned their creation originally. When the partnerships focus on reforging their foundations through better collaboration and clearer objectives, they will be well positioned to design and implement improved procedures.

Technology can be enhanced to better utilise, aggregate and interrogate the data that we generate on financial crime. Currently, too much of the data being generated remains siloed and inaccessible. The financial crime community should accelerate work to aggregate multiple data sources and have them contribute to a detailed map of criminal operations. This will increase the production of the true-positive STRs that we are aiming for. Enhancing our approach starts and ends with partnerships collaborating more productively – and across borders, like the criminals themselves – and committing to the improved use of data, technology, and effective systems to find those true positives.

There are better approaches out there. We just need to be brave enough to challenge our reliance on the traditional approaches that may have made sense when they were created but are now so out-dated as to be almost worthless. We need to innovate and take risks to enact effective prevention of financial crime. Simply fiddling with the existing model will ensure the criminals continue to win.

All opinions expressed here are Tom’s own.

GERALDINE LAWLOR

GLOBAL HEAD OF FINANCIAL CRIME, KPMG

Geraldine is known for her leadership in financial crime having worked in a range of related roles covering advisory, global oversight, standard setting, and operational design and delivery. Prior to joining KPMG as their Global Head of Financial Crime, Geraldine was the Global Head of Financial Crime for Barclays plc responsible for the global design, implementation and delivery of an effective Financial Crime risk management strategy and policy framework.

Throughout her career Geraldine has represented the bank and the industry on several working groups predominately in the UK, Ireland, and Europe. Over 15 years, she has chaired various financial crime related committees at industry level and prior to joining KPMG was the Industry lead on the Government led Economic Crime Reform programme. Geraldine was a founding member of the management board of the Joint Money Laundering Intelligence Taskforce (JMLIT) and the UK Industry lead for the Anti Money Laundering arm of Five Eyes Law Enforcement Group (FELEG).

In addition to above, Geraldine acted as an independent non-Executive Director to an Insurance Syndicate at Lloyds of London chairing their Audit Committee.

I entered the world of financial crime in 2003 and it has been an ongoing voyage of discovery and a passion for me since then.

In the 19 years, I have seen Financial Crime evolve from a laser focus on technical compliance to one that recognises the need to demonstrate effectiveness in mitigating the risk of being used to facilitate financial crime. However, both are not always aligned in outcomes.

I have held leading roles in managing financial crime programmes within both tier 1 and tier 2 banks. Alongside this, I have worked at an industry level in Ireland, the UK and Europe, chairing financial crime related working groups and bringing the conversation on day-to-day matters, as well as on reform, to different regulators and law enforcement agencies. It has been such a privilege and pleasure to work in this area, particularly when I see our work result in real disruption to criminal activity. I have enjoyed immensely this side of banking and continue to do so from consultancy.

My role in KPMG has allowed me to continue supporting firms in their financial crime programmes, whether to meet their regulatory commitments or to transform and optimise. As Global lead partner for Financial Crime in KPMG, I also get to support other member firms with their clients. As I said, it is a privilege.

Let's get 'costs' out of the way

Over the last 20 years the costs of compliance have risen exponentially. Senior leaders are realising that managing financial crime risk requires continuous investment to just 'stay even', never mind the desire to get ahead. Despite all the investment, mainly driven by regulatory pressure, it appears as if it is still not enough, as the value of illicit funds flowing through the financial system is not acceptable and more needs to be done to drive effectiveness.

There is a recognition that this continued investment cannot be sustained and consequently we are seeing a move towards cost optimisation, focused on process re-engineering that drives a more interconnected programme, which is data led and technology enabled. That is where more mature organisations are going and where, for now, the future lies, but it requires some brave decisions on legacy infrastructure, a move out of silo mentality and a bringing together of an organisation in how it views and manages this risk. What some would call a paradigm shift, for others it's just a necessity.

Let's talk about data and technology

How do we create a more effective program and take cost out of the system at the same time? They may look like competing agendas, but if you overlay the opportunity that technology and data presents, you can deliver on all of this and more.

Working in siloed teams for KYC/ CDD, Screening and Transaction monitoring limits the ability to see where transformation can be delivered, which is through a re-architected and interconnected environment, leveraging better data and technology.

With a big focus by regulators and policy makers on technical compliance aligned to demonstrating effectiveness in disrupting financial crime, alongside an internal agenda on cost optimisation, the focus on transformation has never been stronger.

The traditional limitations on data emanating from product led legacy systems are being negated through tools that leverage and enrich existing data sets allowing them to be used more effectively. Banks are also moving from traditional approaches to monitoring transactions into monitoring networks of activity, connecting up relationships and seeing illicit activity across a network that was not evident at a transactional level.

The focus on data is becoming a core and fundamental part of how organisations better manage their FC risks and their KYC / CDD programme lies at the heart of this. Rather than see it as an exercise in ID&V and delivering technical minimums, it should be viewed as the data source to manage all subsequent downstream processes that support better detection, disruption and from a cost perspective, optimisation.

What does convergence look like?

Economic crime is the emerging label attaching to a collection of risks in the financial crime space; namely fraud, money laundering, counter terrorism, market abuse, sanctions, bribery and corruption, and tax evasion. It is a means by which organisations are starting to recognise that managing risks in isolation is not the answer and the future requires a new way of assessing how to deliver better effectiveness as well as drive towards greater efficiency.

We see convergence with fraud and cyber enabled crime moving closer to anti-money laundering particularly around mules. We also see money laundering in markets closer aligned to trade surveillance, where there is opportunity to share insight and tools to better manage risk in the markets business. The same for ESG, where the Environmental, Social and Governance aspects have a direct correlation to threats being considered as part of a financial crime programme with governance having a direct line to the core programmatic elements needed to manage corporate criminal liability programmes, an area that financial crime teams are very experienced in.

So, with a mindset shifting to the need for greater collaboration as a better way of working supported by access to enriched data, information and intelligence, enabled by better tools, the ability to manage risks and threats at a firm level are improving.

"

The loss and harm to society needs to stop and our economies need to be able to prosper and grow. Taking down serious and organised crime will be critical to achieving this.

GERALDINE LAWLOR

GLOBAL HEAD OF FINANCIAL CRIME, KPMG

Let's not forget the regulator

When it comes to Financial Crime, the roles of law enforcement, regulators and industry do intersect; with industry having a role to play in prevention and disruption, as well as detection and reporting.

In the UK and other jurisdictions, regulators are playing a role in supporting, nay encouraging, innovation in identifying solutions to better manage the negative effects of financial crime.

Working with regulators in this way is important. As organisations start to improve the way they respond to and work with their regulators, these relationships will evolve positively. When you start to bring them into the conversation, there becomes a real opportunity to drive a much healthier relationship where we are all on the same side, part of an eco-system that is working together against the common threat, the criminal.

Three lines of defence

With the focus on cost optimisation, the role of the compliance function is evolving. We see a trend towards moving more activity out of compliance and into operations to align to the three lines of defence model and enterprise-wide risk management principles. Moving activity into a shared service allows firms to drive operational standardisation and leverage common tools and management structures.

However, this transition can have its challenges and it is important to set clear outcomes, good design principles and agreement around how accountability, responsibility and oversight needs to work. It is, however, worth the effort as it brings an organisation together, lands accountability with the business for client risk, allows compliance to be the standard setter and move to an oversight role whilst at the same time driving an optimisation agenda through operations, leveraging data and technology to full effect. It sounds easy but it's not.

What about reform?

For several years now 'reform' has been on the agenda with the realisation that we need to approach how we tackle illicit finance and organised crime in a more collaborative way. Working collaboratively internally is important but so is the need to work across industry and with public stakeholders. Public Private Partnerships are a growing theme jurisdiction by jurisdiction. However, underpinning the effectiveness of these partnerships is the ability to share information and intelligence more routinely and with purpose. This is an area where much work is underway as without it the ability to join the dots across the financial marketplace and ultimately disrupt networks of criminality remains limited.

I continue to remain optimistic that true reform in this area is achievable. However, it is hard, with multiple conflicting priorities across the eco-system, but it must be worth the effort. Success will be driven by the will of all stakeholders to change and evolve collectively, and it is amazing what can be achieved when everyone pulls in the same direction. The loss and harm to society needs to stop and our economies need to be able to prosper and grow. Taking down serious and organised crime will be critical to achieving this. Maybe, the ESG lens is the one that drives the momentum to finally move us forward to where we need to be. I do hope so as we cannot stay where we are.

All opinions expressed here are Geraldine's own.

MICHAEL LEVI

PROFESSOR OF CRIMINOLOGY
CARDIFF UNIVERSITY

Professor Michael Levi is a distinguished and esteemed subject matter expert in financial crime, winning major international prizes for his comparative work on economic crime. His research and contributions to the field of criminology focus on the links and incongruities between white-collar and organised crime, and how the activities executed within each can be more effectively controlled.

He has contributed numerous publications studying money laundering in relation to drug crime, fraud and cybercrime and holds many public positions across domestic and international committees such as the UK Cabinet Office Counter-Fraud Cross Sector Advisory Board, Europol and the EU Group of Experts on Corruption.

Background

My research in money laundering is primarily motivated by the desire to understand the involvement of financial activity in fraud and white-collar crime. After the Brinks-Mat robbery of 1984 and a superficially minor fraud scandal in 1988, I was asked to provide a review of the control of these financial crime activities. The review revealed an obvious network of responsibility to cooperate between banks and police which was not being adequately performed.

Even as regulations were being introduced dictating the expectations of banks and police to investigate suspicious financial activity, competing objectives and procedural challenges marred the success of what we know today as financial crime compliance (as I discuss in my work *Pecunia non olet: Cleansing the money-launderers from the Temple*, 1991). The current compliance activities are useful in reducing the likelihood of banks being fined or reprimanded but have not demonstrably done much to reduce any forms of crime or to mitigate how 'organised' they are. This begs the question, what can we do differently to address the issue that we only disrupt 1-3% of known crime for economic gain?

Threats and challenges

I have noticed there is a tendency to focus on new threats before the current threats are adequately addressed. Thus, although services-based money laundering is a problem, we have not yet developed an effective response to trade-based money laundering, so does it make sense to focus on the former rather than the latter? Criminals will simply continue to exploit the current vulnerabilities which we are not controlling, without a need to adopt new practices such as service-based or crypto money laundering.

Crypto will inevitably be a future threat because it is a less traceable form of money. However, it is only a suitable method in some markets and

will not be exploited by the criminal operations which rely on more tangible movements of cash. The prevalence of the threat will greatly depend on its benefit and utility to different criminal markets: the sooner we develop our understanding of market intricacies the better able we will be to gauge new threats. And we need to distinguish between using crypto for money laundering and thefts of and from crypto exchanges (which themselves may need to be laundered).

Responding effectively

I am glad to see a shift away from the 'follow the money' organised crime control assumptions of the Reagan era into a more problem oriented policing approach. This has facilitated better allocation of resources in AML efforts to support intelligence gathering and sharing, especially with SARs. One of my concerns over the current system though is the gross underutilisation of SARs. For the amount that is invested into this capability by various entities, there needs to be more certainty that the regulator and/or criminal justice agencies are capitalising on the intelligence. Thus 'responsibilisation' of the private sector needs to be accompanied by public investment if it is to pay off.

Apart from the conception of the Financial Action Task Force (FATF), I don't believe there has been a real paradigm shift in AML to date. This is not to say there have not been beneficial developments over the last few decades, but I believe these advancements were not as strong as they could have been. There is an opportunity for new practices to be forged, potentially in the way of international data-sharing and technology leveraging, to influence a systematic change for the better in AML. The current system of designating country (non) cooperation has a legitimacy and fairness problem and should be reviewed to hold jurisdictions accountable for their AML actions, relative to economic size and importance to illicit flows, for example. That would serve as grounds upon which a paradigm shift in better practices could unfold.

Public private partnerships

The future of public-private partnerships depends greatly on what entities need, legally can and are willing to do. I believe the partnerships and SARs are good efforts in AML. But at the moment, tectonic plates of data privacy and AML efforts clash in many parts of the world with not enough being done to improve on anonymisation via Privacy Enhancing Technologies and sharing of information. People and entities need to be willing to change and trust each other before this produces a step-change.

Those entities comprising partnerships need to invest in data optimisation to ensure they are sharing meaningful information. Part of improving the quality of data and ability to share involves removing barriers caused by privacy restrictions through de-identification. Even when data is anonymised, it can unveil connections across institutions or suspicious operations which we are otherwise blind to without cooperation facilitated by those partnerships. Better data also involves improving visibility of suspect finances in other sectors such as accounting and law firms.

Regulators can be clearer and more conscientious in their advice on risks. Jurisdictions have their own challenges and range of vulnerabilities with varied level of risk, requiring unique responses. The regulators should support the entities in devising a best practice approach for their circumstances, rather than prescribing a sometimes arbitrary and ineffective risk checklist across the board.

Compliance costs

For banks specifically, there will always be a cost-benefit assessment of investment in regulatory activity and compliance over the risk of financial and/or reputational sanctions. The risks of fraud to the financial sector directly and via reputational risks have grown apace in the last few years, but it is not clear how much banks and other regulated bodies would spend on compliance, absent threats of criminal or regulatory penalties. Pragmatically the banks will have to keep spending money in AML and so it is in their interest to invest wisely, optimising their data and technology for quality insights. For some banks, there may be a greater willingness to tolerate the risk of non-compliance penalties – but even this will ultimately incur costs. The banks should simply behave better: how far this normative perspective and cultural expectation would be translated into corporate spend is a matter of dispute. But at least institutions should not be required to spend large sums on activities that have no clear benefit.

All opinions expressed here are Michael's own.

"

We will be better at addressing the problem when we do more critical thinking and less arbitrary reacting.

MICHAEL LEVI

PROFESSOR OF CRIMINOLOGY
CARDIFF UNIVERSITY

David joined the FATF in 2015, following posts for the UK Government as Head of the Illicit Finance Unit and Senior Policy Advisor at HM Treasury, and before that as a senior member of the Serious Organised Crime Agency (now National Crime Agency).

He has a broad range of other experience including at NGO's and in the public and private sector, from leading and supporting expeditions in the rainforests of Indonesia, to working on some of the largest initial public offerings and government privatisations and managing the digital product portfolio of the UK national mapping agency.

David has a BA (Hons) from the University of Portsmouth, MSc from Cranfield University and is a Fellow of the Royal Geographical Society.

In his role at the FATF, David is responsible for leading the FATF Secretariat in bringing to bear the combined expertise of governments around the world to fight money laundering, the financing of terrorism and the proliferation of weapons of mass destruction.

This includes work to monitor how money is being laundered and terrorist organisations are raising and accessing funds; to develop global standards, best practice, and guidance to mitigate new and emerging risks; and to assess the action taken by governments. It also includes providing training and support for officials from FATF member countries and the nine FATF-Style Regional Bodies.

Enhancements in our efforts to combat money laundering and terrorism will come when we move beyond compliance to being purpose-driven and intelligence-led. This will drive a more effective system, with public-private partnerships as core, which will allow us to focus on combatting serious and organised crime that affects our community.

We need to come back to why we do this. My concern is that one of the reasons we are collectively doing so badly is because the goal of protecting the integrity of the financial system does not motivate people. Anti-money laundering and countering the financing of terrorism is about reducing the harm caused by crime and terrorism. Full stop.

DAVID LEWIS

FORMER EXECUTIVE SECRETARY,
FINANCIAL ACTION TASK FORCE (FATF)

I joined FATF from the UK Serious Organised Crime Agency (now National Crime Agency) and could see that following the money is the best way to fight serious organised crime. In this industry, if you do not get up in the morning looking to stop harm from serious and organised crime, then you are kind of missing the point.

The role of the supervisor is critical but the global approach to regulation is nascent but underdeveloped. The FATF's evaluations have found that 25% of countries have a good level of effective supervision, however 75% still have a big uphill climb. Regulators have been appointed a complex job which requires an expertise in risk. Risk-based supervision will ensure that banks are putting their resources in the right place, but that is just the beginning of the improvement we need to see. The rest of it will need to come from intelligence-led supervision, and this starts with public-private partnerships.

The progression of public-private partnerships will vary globally – there will never be a one size fits all approach. One of the challenges around making these work is finding the people you can really trust. Combined with this, we need to look at expanding the role of information sharing at cross-border levels and doing this in a way which respects data protection and privacy. We are trying hard at FATF to engage with data protection authorities, including at an EU level, but it has been difficult. The oldest quote in the book is "criminals have no respect for borders", and we must do the same.

Innovation in technology will not just come from private sector, law enforcement or regulators – it will come from technology innovators, the next generation who wear t-shirts to work and understand what can be done with technology. What is starting to show is a difference in understanding between banks and technology innovators. Technology innovators think that all they need to do is provide the technical solution to what the banks already do, but the problem is what the banks already do in many cases is ineffective. We need to build an understanding of what the problem is and the motivators for this issue.

The investment in people, technology and processes will only be effective when we have a supporting culture, that ultimately needs to come from the top. You can have a million people working on compliance, but these people need to be incentivised to ask the right questions. This is not about compliance – the efforts involved to identify suspicious activity is good for your business, protecting brand and reputation. A lot of it comes back to cultural change and understanding why we are doing this. In terms of tackling that culture now, we all need to start talking the same language. This is not just about financial integrity – it is about reducing harmful crime and terrorism. For too long conversations that have been occurring at the level where it matters have been the wrong conversations.

To prepare for the future, regulators and law enforcement need to get into a room with the big banks and draw out on a wall what financial crime will look like in 5 to 10 years' time. They then need to develop a roadmap that will help them get there. A risk-based approach may not mean cutting everything from the current process, and there are some technical, legal, and cultural challenges that we will need to overcome – this is a multi-year effort.

I hope that FATF will also continue to progress in the right direction. The good news is that we have 205 jurisdictions which agree on the FATF Standards who should be able to get on with it with no excuses.

All opinions expressed here are David's own.

"

To make progress we need to come back to why we do this. This is not just about financial integrity – it is about reducing the harm caused by crime and terrorism. Full stop.

DAVID LEWIS

FORMER EXECUTIVE SECRETARY,
FINANCIAL ACTION TASK FORCE (FATF)

IAN MCCARTNEY

DEPUTY COMMISSIONER
AUSTRALIAN FEDERAL POLICE (AFP)

Deputy Commissioner Ian McCartney has been a member of the Australian Federal Police for 30 years. Prior to joining the AFP, Ian worked as an accountant, obtaining the status of Certified Practicing Accountant. Ian has diverse experience with the AFP in national and international economic and organised crime investigations and has participated in a number of taskforces involving Federal and State law enforcement agencies.

Ian was awarded with the Australian Police Medal as part of the 2014 Queen's Birthday Honours in recognition of his distinguished service, particularly in the areas of law enforcement liaison in Asia, and for his role in national investigations. Ian is the current Co-Chair of Asia/Pacific Group on Money Laundering.

I was a Junior Accountant before I joined the AFP over 30 years ago and was placed to investigate sophisticated economic crime organisations. Most of my early work in the AFP involved complex offshore taxation fraud, which was a technically challenging but rewarding environment to work in. Financial Crime is a silent but insidious crime, with the impact ranging from democratic institutions to vulnerable people who are targeted. I am motivated every day by the fact that I get to protect our community and keep Australia safe.

The AFP has had to change from a capability, cultural and strategic perspective in the way we talk about targeting organised crime. When I first joined the AFP, we did not use computers and every crime we investigated was in the real world. Today crime is heavily based online, which creates a challenge for us but also opportunity.

Risks and Threats:

When I joined the AFP the biggest threat of organised crime was from criminals based in Australia. Today, much of the organised crime impacting on Australia is perpetrated by criminals located offshore, in jurisdictions where it is challenging to investigate.

We know that organised crime needs 3 things to operate: the logistics to move the product, the financial services to place the money, and free communication to organise the purchase.

The sophistication of online organised crime will continue to increase. The level of violence in organised crime syndicates is concerning, and on a global scale. The number of child sex offenders since COVID-19 has become more prevalent. Physical cash is reducing, and the use of digital currency and online payment platforms increase. The ability to move funds faster and hide those funds more easily will challenge law enforcement.

“

We took a considered risk with Operation Ironside and embedded financial institutions into our own site to help us with the data analysis for the operation, and this was critical to its success.

IAN MCCARTNEY

DEPUTY COMMISSIONER
AUSTRALIAN FEDERAL POLICE (AFP)

If we can disrupt the supply of money laundering offshore, then it has a direct impact on the criminality we see onshore. As we look to the future, the best way to define success in the next 10 years will be making Australia a hostile environment for offshore criminals to operate in.

Operation Ironside Lessons Learnt

We took a considered risk with Operation Ironside and embedded financial institutions into our own site to help us with the data analysis for the operation, and this was critical to its success. We brokered a relationship with a bank and sent our officers to learn about their capabilities and methodologies, so that we could better understand how they operate. It was surprising how much we benefited by learning from each other.

Across the public and private sector, I believe we all need to sit down at the same table and realise there is a common purpose. There is a need for cultural change in law enforcement because traditionally we have not shared intelligence. However, recently we have seen green shoot partnerships developing with opportunities to collaborate for a common purpose. The key to a solid relationship between financial institutions and law enforcement is trust on both sides. This will allow us to become better at providing feedback which will lead to better outcomes.

Our investigations involve detecting whether criminality has occurred. The AFP is very good at asking financial institutions for support but then we quickly move onto the next job. We need to improve the way we articulate the impact of financial institution's assistance if we want to progress the feedback loop.

Financial institutions have compliance regimes for the right purpose, and it impacts profits and their brand if something goes wrong. It is important that they understand the value they are receiving from their investment, and the function of the feedback loop that they provide to law enforcement and AUSTRAC that protects the system.

Technology and Data

At the AFP, we have had to continually change our strategy towards how we target organised crime groups, and we need to continue to develop new capabilities which will support our ability to combat financial crime.

Technology can offer these capabilities, however the challenge for law enforcement is big data. The sheer size of material that our officers seize via search warrants is challenging. Often that data is in a foreign language which causes further difficulties. Machine learning will be critical in addressing how we interpret, ingest, store, and analyse that data all in a single system. So far there has not been one product that will solve all these problems.

Private-Public Partnerships

Private-Public Partnerships will play an incredibly important role in how we learn what capabilities are required to analyse and share data, and how we do it. We know that we do not have the full skillset to deal with the challenge of big data, however our ability to learn from financial institutions will ultimately play a key role in the evolution of law enforcement. Banks continue to provide a huge impact, and sometimes I do not think they always understand the impact they make.

All opinions expressed here are Ian's own.

TERRY PESCE

PRESIDENT AND CEO AT TERRY PESCE & CO LLC, FINANCIAL CRIMES LEGAL AND REGULATORY CONSULTING

Terry Pesce is an industry leader in Financial Crimes Regulatory Compliance and Enforcement. She has a demonstrated history of working in and with the financial services industry, including in government, industry, and consulting.

Before forming Terry Pesce & Co LLC, she was a principal in KPMG's Forensic Advisory Services, serving as Global Head of AML Services and Head of Financial Crimes Solutions in the US. Terry served as an Assistant to the United States Attorney in the Southern District of New York where, as Chief of the Major Crimes Unit and Deputy Chief of the Criminal Division she supervised the district's money laundering investigations and prosecutions.

She holds a BA from Columbia University, and a JD from Columbia University School of Law where she served as Managing Editor of the Law Review and received prizes in Constitutional Law and Trial Advocacy.

I believe the prevention and detection of financial crime is important on both a micro and a macro level. Financial crime takes money out of the good global economy and puts it into the hands of the bad actors. The better resourced the bad actors are, the more havoc they can wreak (whether it's terrorism, cyber threats, ransomware or similar), and the worse off we become.

I started working in the field during the 1990s as a prosecutor of money laundering cases where the primary concern was narcotics trafficking and organized crime. I lived in New York during the 9/11 attacks, and we all took a stark look at that point, realizing the importance of terrorist financing, and how much power we could have if this was our focus. I feel very passionately about that. That was really when the paradigm shift occurred for the banks and for regulation.

Lessons learnt

We have learnt a lot but also continue to learn in this space. From the 9/11 attacks, we learnt that the illegal movement of money can have many implications. The attacks were funded with about half a million dollars, which is quite low. The dollar amount doesn't have to be large to have a very big impact.

“Millions of suspicious activity reports are filed every year, but very few are acted upon. In what other industry would a one percent success rate be acceptable?

TERRY PESCE
PRESIDENT AND CEO AT TERRY PESCE & CO LLC, FINANCIAL CRIMES LEGAL AND REGULATORY CONSULTING

We also learnt how to set up programs that are supposed to help us understand: who we're doing business with, what their activity looks like, how we can detect and report suspicious activity, and perhaps keep bad actors out of the financial system. I still don't think we're doing this as well as we could be. These systems are only a partially useful exercise. For example, millions of Suspicious Activity Reports (SARs) are filed every year, but very few are acted upon. There are a lot of investigations that will never amount to any law enforcement action. In what other industry would a one percent success rate be acceptable?

Innovation and technology

I certainly hope the biggest catalyst for change over the next 5 to 10 years will be technology and innovation. There are continuous opportunities to apply or develop technology to create effective change. Maybe the next few years will see a challenging of traditional practices through new ideas and more efficient methods.

In the next 10 years, banks will likely be more open to new ways of working in order to meet regulatory expectations, but in an efficient manner. The current attitude is often 'if it ain't broke, don't fix it', despite many of the current systems being inefficient and ineffective.

Banks are currently reluctant to change their ways because they fear resistance from their regulators, or they simply have no motivation because their current approaches are deemed acceptable (from a regulatory perspective, but not necessarily from a crime prevention perspective).

I think technology is the only thing that's going to save us from increasing and potentially excessive compliance costs, so we must be ready to take that leap. Machine learning, artificial intelligence, and real-time data assessment are critical because relying on mass amounts of people to perform investigations is inefficient.

Data to provide a holistic customer view

I don't believe we maintain a holistic view of the client and all the tentacles that attached to the clients. If we could get rid of all the noise, we could get quality insights by looking at what's really unusual activity for a particular customer. While certain data points can be shared, they are often not the ones that are that useful. You can't share underlying transactional activity, and banks are not going to share their policies and procedures around what pieces of information they're collecting.

Having good data is key. There needs to be an assessment of data lineage: making sure that the data itself is clean and complete, and then there needs to be a reconciliation to get rid of all the old information so what is reviewed is current and accurate. To generate a more holistic view there should be an active link between transaction monitoring and KYC, ensuring it is constantly updated for real-time insights.

Future direction

I really think organisations need to take a top-down approach and restructure with a different focus. The amount of information that organisations collect is huge, and don't necessarily tell you enough about the entity you're dealing with to make it meaningful. We need strategy teams that are thinking about how we can do this differently - more effectively and efficiently. Instead of just ticking the boxes, we need to be solving the problem.

All opinions expressed here are Terry's own.

JIM RICHARDS

FOUNDER AND PRINCIPAL
REGTECH CONSULTING

Jim Richards is the Principal and Founder of RegTech Consulting, a private consultancy aimed at developing the next generation of BSA/AML and financial crimes professionals, technologies, and programs. Prior to founding RegTech Consulting, Jim worked for almost 13 years at Wells Fargo & Co. as the BSA Officer and Global Head of Financial Crimes Risk Management. He was a founding member of ACAMS Advisory Board, a three-time member of the Treasury Department's BSA Advisory Group (BSAAG), and the author of "Transnational Criminal Organizations, Cybercrime, and Money Laundering" (CRC Press).

I had spent some time with the Royal Canadian Mounted Police and as a prosecutor, so fighting against crime in general was something I always had in me. After my family was threatened by a mobster in Boston during my time as a prosecutor, I decided to take up an opportunity to become an MLRO equivalent at a bank in Boston. Whether in the public or private sector, prevention of financial crime is crucial to keeping our families and our communities safe. For me, I never would have ended up in banking but for the MLRO role. And it's a role that is always changing: the financial crime space requires transformation and change as criminals have the ability to move faster than us and we don't know if we will ever be able to keep up.

Data and Technology

The key to private sector financial crime efforts is using all the data you have as efficiently and effectively as possible. But I don't think we've done a great job utilising data or technology. It is essential financial institutions clean up and manage their data, as it is key to getting financial crime right. Once we get the data right, the real change, especially for big banks, would be to utilise fit-for-purpose specific fintech solutions. With traditional off-the-shelf customisable systems, banks cannot adapt and react as quickly as they need to.

Another way to look at making AML more effective and efficient is to look at AML as marketing in reverse. Marketing is finding out who our target audience is and how we identify them, get them through the door, learn as much as possible about them, and keep those customer relationships. The skills, procedures, technologies, and data that bankers have and use for finding the best customers could be used to find the worst customers. We just turn it around to ask: how do we identify the customers we want and don't want, how do we monitor unfavourable customers, and how do we exit them? So maybe the sales and marketing departments in your bank have solved your AML problems!

Or perhaps the private sector financial crime compliance community can learn from non-financial organisations like Google, Amazon, Netflix, and Facebook. Maybe they have already solved the financial crime problem from a technology perspective with their ability to take in, understand, and use data. They take all their user's data and can identify which adverts to put in front of you, or which products you might want to order, or which movies or music you would like. Perhaps financial institutions can do the same thing, but for a different purpose: to identify money laundering and terrorist financing. It's worth a try because what we're doing today isn't working well.

Risk and Regulatory Response

Evolution or revolution sums up how this industry changes. Fintech companies are all about revolution: they are agile and deliver value quickly. The other revolution which we tend to have every couple of years are event-driven elements like the Panama Papers, the Paradise Papers, the Pandora Papers, the AUSTRAC enforcements in Australia, and the Danske Bank issues in Europe.

But on the back side of revolution is the regulatory response that is always an evolution. The frequent revolutions that occur make it very difficult for regulators to evolve quickly. The slow cycle of regulatory evolution and legislative change needs to pick up pace to keep up with the multiple revolutions.

Over the last 15 to 20 years, national regulators have imposed increasingly complex compliance requirements on private sector financial institutions. The original intent of AML regimes – providing law enforcement with timely, actionable intelligence – has been overtaken by what is known as 'check the box' compliance. A real threat and vulnerability in the financial crime space is a singular focus on the foundational aspects of compliance at the expense of providing intelligence to law enforcement.

I believe Australia and the United States have the same issue. And the United States has made it even more difficult for financial institutions to meet their program requirements, because those requirements come from four different titles of the U.S Code. Those four titles – Title 12 (the banking laws), Title 18 (the criminal laws), Title 31 (the so-called Bank Secrecy Act), and Title 50 (the sanctions laws) often conflict. I call it "The Clash of the Titles".

> "
>
> **The private financial sector has been seconded by the public sector to assist the public sector in the fight against financial crime.**

JIM RICHARDS
FOUNDER AND PRINCIPAL
REGTECH CONSULTING

Public Private Partnerships

AUSTRAC have started doing a better job in getting feedback to financial institutions. However, the AUSTRAC's and the FinCEN's of the world need to start providing more actionable, specific feedback on which specific reports submitted by a regulated entity actually add any tactical or strategic value to law enforcement. Financial institutions can then start tuning their systems using machine learning and artificial intelligence based on the intel received.

We are on the up slope of private-public sector partnerships - it is a great idea, and we are starting to do more, for example, the Fintel Alliance in Australia. However, as long as financial institutions are primarily judged on the strength of their compliance program and not on whether they are providing timely, actionable intelligence to law enforcement, these partnerships will level out, or even collapse.

How can we make the necessary regulatory changes? Over the next 5 to 10 years, financial crime regulation needs to be more outcomes-based rather than inputs or outputs-based. Inputs are all the things that go into a program, such as risk assessments, policies and procedures, and onboarding customers appropriately. Outputs are all those reports that are filed such as SMRs or STRs, large currency reports, and wire transfers reports.

Outcomes, however, are the arrests, convictions, seizures that result from the inputs and outputs. After all, the ultimate goal is to prevent and mitigate the effects of crime and terrorism, not to have good policies or to file lots of SMRs.

Compliance Costs

The financial crime space is ever evolving, and financial intuitions need to be resilient and adaptable, which comes at a cost. Financial institutions are solving yesterday's problems with remediation and are stuck with systems that are not fit-for-purpose. They are not setting up for success in the future, and even if they are, the future changes.

The cost of financial crime compliance isn't going away. The best way to go forward is spending money right and leveraging what has been spent. And being judged on the true outcomes.

The Future of Financial Crime

Even though I've focused on data and technology, the biggest contributor to the paradigm shift in combatting financial crime is the people. When I started in the industry 4 decades ago, my young peers and I were completely unprepared, overwhelmed, outgunned, and outmanned. This generation is so smart and dedicated – an altruistic, clever, and collaborative generation that realizes we can do well and do good. I am very optimistic that this generation will shift us to an outcomes-based regime that will effectively and efficiently protect our families and communities from financial crime.

All opinions expressed here are Jim's own.

Sarah currently works for Facebook in Washington DC as a Director for Global Payments. Previously, she was Global Head of FCC Regulatory Strategy with Credit Suisse, and before that worked in the Office of Strategic Policy for the U.S. Department of Treasury.

Over the last decade, I have enjoyed discovering how relevant fighting financial crime is to the global community, and where it is making an impact.

I am a naturally mission-oriented person due to my background in government. Financial crime lends itself to mission driven people who are both tactical and strategic.

What I have missed the most over the past two years is travelling to conferences and meeting other members of the AML community, because when we have that time together, it can be very productive as we share stories and problem solve together.

Financial Crime Evolution

There have been some important evolutions over the last few years. But why is there still so much financial crime? Why are we not seeing the problem dissipate?

The answer is that you can have the best rules in the book, but unless they are applied effectively, the rules do not matter.

Current global dialogue regarding the importance of an effective regime stems from FATF's effectiveness criteria. The industry agrees that a paradigm shift to version 2.0 is required, but governments need to be willing to accept the risk of failure to help us make that shift.

Over the last 5 years, active enforcement combined with FATF's effectiveness criteria has had a positive impact. It will be interesting to witness where FATF is heading in the next round of evaluations and how this will push countries to pivot. The influence of FATF has grown tremendously and is changing behaviour at the country level and in industry.

Public-Private Partnerships

Public-private partnerships have been a great addition to the tool kit in the fight against financial crime but there is scope for them to become more meaningful.

SARAH RUNGE

DIRECTOR, GLOBAL PAYMENTS, REGULATORY, FACEBOOK

There is value to providing targeted information and typologies. Information sharing outside of jurisdictions is challenging because of data sensitivities, but typologies allow more participants to join at the table. However, typologies are often very broad, and part of refining the detection process will be asking ourselves – what are we trying to get out of it?

At the same time, governments, law enforcement and policymakers need to get into a room together and ask – what do we want to achieve through these frameworks? Because this is not just about prosecuting bad actors but also identifying illicit proceeds in the first place.

Suspicious Activity Reports

We need to implement a more effective suspicious activity report (SAR) regime. The use of data and artificial intelligence will be a big part of generating more targeted valuable SARs. However, the other part is an appetite from the government to support new approaches.

The US file more SARs than any other country. But at times, this can be simply because it is easier to submit a SAR than to explain why you did not. Implementing straight-through processing, without human intervention in some cases, could have an impact on our ability to focus on meaningful information.

Data

Good data is key, and the vast majority of financial institutions have massive challenges with data, however in my experience firms seldom invest anywhere near as much as they need to fix the root cause of poor data.

Any capacity to monitor your transactions effectively is dependent upon the quality of information you collect in the first instance, as well as how that is maintained and shared globally. Ultimately the quality of your data is based on how well your on-boarding procedures are to identify and verify information and subsequently accurately risk rate your client.

Technology companies are fortunate because their financial data is more integrated. Any global bank that has grown and acquired other institutions, but never invested in consolidating or formatting their data, will find that getting that data together now will be challenging, time-consuming, and costly. Technology companies are constantly testing their own data, outside of audit or quality assurance checks, but as business as usual.

Cost of Compliance

There is a risk that we maintain a view that the private sector has endless resources, and we can solve any problem, and we absolutely cannot.

There are large global US institutions that have thrown everything they have financially at these problems, and yet have still been under enforcement for many years.

There is no limit to how much an organisation can spend on financial compliance. However, we need to step back and re-imagine our compliance program, because fixing broken things with tape will inevitably fail.

All opinions expressed here are Sarah Runge's own.

> “
>
> **We need to step back and re-imagine our compliance program, because fixing broken things with tape will inevitably fail.**

SARAH RUNGE

DIRECTOR, GLOBAL PAYMENTS, REGULATORY, FACEBOOK

Liat is a financial integrity professional with over 15 years of experience in strategic research, program development and organisational leadership across Africa, the Middle East and the US. Liat has previously worked as the Senior Advisor for Crypto-Policy and Regulation at blockchain analytics company Elliptic, and in the AML/CTF space at the Egmont Centre of FIU Excellence and Leadership (ECOFEL) and the European Commission. Her expertise includes RegTech and FinTech, and AI-based solutions for CDD.

Financial crimes hurt lives, children, families, and communities. They disrupt society and take resources away from those who need it most. I spent 15 years in the Horn of Africa helping with anti-money laundering and financial inclusion projects, particularly helping women to find access to promote their businesses. Having worked across financial inclusion and combatting financial crime, I have seen first-hand the importance of increasing access to financial services while keeping the bad actors out.

Lessons learned for the future

We've learned that we need to be faster at embracing technology into our workflows, because current practices are simply not fast enough. We need to make our procedures and workflows more efficient and effective, and we need a solid integration between technology and human intelligence. We shouldn't assume tech or humans alone can address today's challenges, instead we need humans to work with technology to make processes better.

We need to do more to equip our law enforcement and investigatory capabilities with technologies to find and share information quickly in investigations. Data is spread across jurisdictions, entities, institutions, and stakeholders - we need to overcome data fragmentation and combine it with speed and effectiveness. Finding the needle in the haystack should be a speedy process.

We have also seen that corruption remains malignant globally, we need to understand it will always be here. It's in all centres of finance, and we can't ignore it. This is why it is so important to integrate environmental, social and governance (ESG) factors into finance.

LIAT SHETRET

DIRECTOR OF GLOBAL POLICY AND REGULATION – ELLIPTIC

Challenges and future change

Our biggest challenge in combatting financial crime is establishing digital identity. Specifically, the identity between our online and offline personas. There are issues around vetting and authentication of a digital identity that have been brought on by the pandemic and digitisation. This introduces challenges around proving customer authenticity, or proof of ownership over assets. The challenges exist for individual digital identity, the digital identity of companies, shell companies and beneficial owners of funds and assets.

Blockchain technology can help in this regard. Digital assets on the blockchain essentially allows you to demonstrate provenance at a particular time, on a particular day – it's stamped in. However, this doesn't get rid of corruption. I think blockchain offers opportunities to make financial crime compliance more efficient by vetting the information that comes in.

Banking & cryptocurrency

We must get a handle on crypto exposure impacting banks and other financial institutions – it's here, it's not going anywhere, and it's deepening. Banks must get on board whether it's to become custodian institutions themselves and apply the compliance and regulatory playbook to that line of business, and to make sure that the financial crime risks associated with crypto are appropriately mitigated.

For banks, the biggest fear around not embracing crypto and digital assets is losing a line of visibility that is critical to risk management and exposure. Using traditional methods of financial crime detection and prevention, all the banks see is money coming and money going. This does not show what is happening on the other side (e.g., child exploitation, buying fake IDs, selling arms). However, there are tools already available today that go beyond this.

There's no integration with legacy systems, there are so many departments and the data doesn't speak to each other and is non comparable. Banks are going to have interoperability functionalities with crypto exchanges and vice versa. There must be a line of vision in the digital space that connects customer activity with traditional finance and this new crypto business. The KYC needs to straddle traditional finance and the cryptoverse. Data is the new holy grail. Datasets need to be comparable, and speak to each other, so we can generate critical insights. This is my favourite part and it's why I worked for a blockchain analytics company such as Elliptic.

A bank would need to update their risk assessment for crypto exposure, and they need to have the software to implement it. The laborious element of intelligence and threat hunting is made redundant by shifting into crypto because as an open blockchain based on ledger technology, following the money is so beautiful and simple.

Regulators

I think the receiving end of suspicious activity reports (SARs) on the regulatory side is where we're going to be seeing a difficulty in that paradigm shift because they're often under-resourced, underpaid, and understaffed. Regulators need the right resources to identify issues and investigate information that comes from all the reporting entities. There will also be new reporting entities coming into play with digital players because they're now also responsible to submit SARs, which you know is another huge amount of data to sift through.

Financial crime regulators are going to need to invest in technology. They are going to need to develop a two-way communication stream where they are not only receiving information, but also quickly communicating back out to the industry what their expectations are around red flags as well as trends they are seeing. It's almost like they need to conduct meta-analysis levels for all the data, because they're the only ones with a view of the entire landscape – whereas every individual bank or entity is kind of on their own.

Public-private partnerships

Before we get to public-private partnerships, I think our main issue of today is public-public partnerships. There's a lack of clarity around who does what in the public sphere. We need to establish clarity on what information public sector actors need from other public sector partners to do their job. There should be an inventory of what current public sector actors need before the private sector can step up to initiatives. The workflow is slow and cumbersome and for private sector companies to effectively contribute resources, government agencies need to be clear on what it is they need.

All opinions expressed here are Liat's own.

> "We must get a handle on crypto exposure impacting banks and other financial institutions – it's here, it's not going anywhere, and it's deepening.

LIAT SHETRET

DIRECTOR OF GLOBAL POLICY AND REGULATION, ELLIPTIC

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 with the following:

- Developing strategic roadmaps
- Implementing our global perpetual KYC solution
- Developing and executing a technology strategy
- Sharing expertise on innovative customer monitoring
- Providing global better practice insights and intelligence
- Optimising and digitising Financial Crime Operations

Acknowledgements

This report was very much a team effort. A special thank you to Demi Lari, Nada Jevtovic, Miriam May, Katherine Robinson, Lachlan Hardisty.

Contact

Sue Bradford
Partner
T: +61 415 246 076
E: suebradford@kpmg.com.au

Warren Dunn
Partner
T: +61 411 755 595
E: warrendunn@kpmg.com.au

Alexander Graham
Partner
T: +61 406 614 739
E: agraham@kpmg.com.au

Timothy Goodrick
Director
T: +61 2 9455 9773
E: tgoodrick1@kpmg.com.au

Ben Meager
Director
T: +61 431 291 020
E: bmeager@kpmg.com.au

Mervyn Poon
Director
T: +61 410 637 806
E: mpoon1@kpmg.com.au

KPMG.com.au

December 2022. 1034287909FS