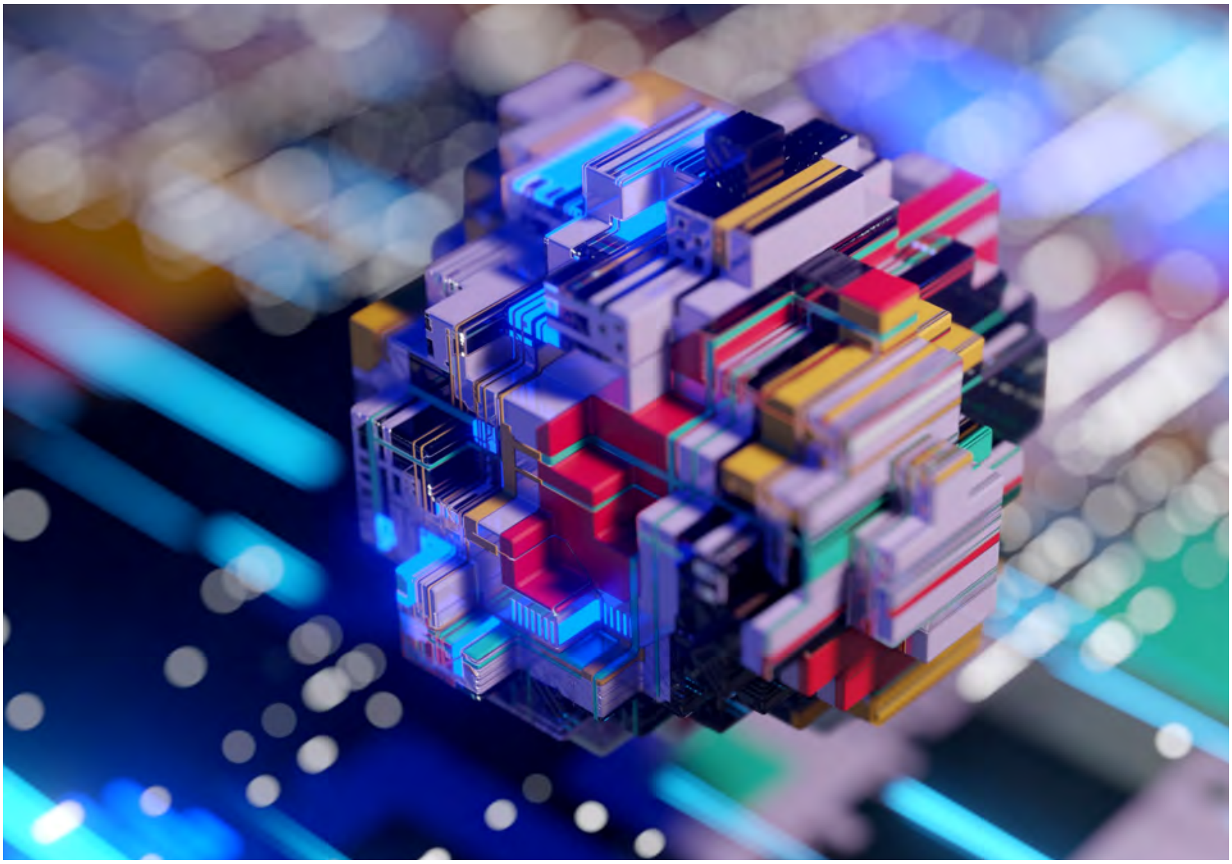
CENTRAL BANKING
FOCUS REPORT

Anti-money laundering and countering the financing of terrorism



In association with

KROLL

Seeking an edge in the fight against money laundering

Report editor: **Dan Hinge**
dan.hinge@centralbanking.com

Commercial editorial manager: **Stuart Willes**
stuart.willes@infopro-digital.com

Senior commercial subeditor: **Alex Hurrell**
alex.hurrell@infopro-digital.com

Chairman: **Robert Pringle**

Editor: **Christopher Jeffery**
chris.jeffery@infopro-digital.com

Global brand director: **Nick Carver**
nick.carver@infopro-digital.com

Commercial director: **John Cook**
john.cook@infopro-digital.com

Global corporate subscriptions manager: **Michelle Godwin**
michelle.godwin@infopro-digital.com

Cover image:
aislan13/Getty

Technology is reshaping the modern economy, giving people new ways to pay for goods and services, new assets to invest in and even new jobs. Many economists hope that technological change could be a powerful driving force for productivity gains in the years ahead.

But for those focused on fighting financial crime, technology is a double-edged sword. The growth of data and digital channels has gone hand in hand with the rise of new crimes, from cyber attacks to electronic forms of fraud. Technology also gives criminals new routes to make off with the proceeds of crime. Crypto assets provide a convenient, anonymous means to launder money or to fund terrorist organisations.

This special report explores how supervisors are responding – from closer collaboration to new uses of data and technological tools. Our new survey of central banks highlights how many are turning to various innovative forms of data analysis to improve anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts. Many are also working together to share intelligence across borders.

But there is clearly room for improvement, both in terms of technological platforms to highlight AML breaches, and in cross-border co-operation, which is weaker than domestic collaboration. One-third of central banks that responded to the survey do not use data analysis for AML purposes, and nearly 40% say they do not share data on suspicious transitions with counterparts overseas. Many also report that resourcing is a challenge.

One organisation at the heart of efforts to improve digital AML tools and cross-border collaboration is the Financial Action Task Force (FATF). Marcus Pleyer, FATF president, talks to *Central Banking* about what techniques supervisors can use to stay ahead in the race against criminals. He highlights how digital tools can boost the efficiency and effectiveness of AML/CFT measures, and may also help alleviate tensions between oversight and privacy laws.

Crypto assets represent a new frontier in the fight against money laundering and terrorist financing. Bernadette Lee reports on the rise of crypto assets and stablecoins, and asks how AML agencies worldwide are responding. There has been a flurry of activity in recent years, but gaps in regulation remain, and crypto asset services providers may need to step up their own efforts.

Ultimately, the battle between AML supervisors and criminals may never end. "As long as there is money, there will be money laundering," Pleyer notes. All the same, supervisors must do what they can to stay ahead in the technological arms race. ❑

Dan Hinge,
Report editor

Central Banking Publications
Infopro Digital Services
5th Floor, 133 Houndsditch
London EC3A 7BX
Tel: +44 (0)20 7316 9000
Fax: +44 (0)20 7316 9935
Email: info@centralbanking.com
Website: www.centralbanking.com

Published by Infopro Digital Services Ltd

The good, the bad and the ugly: how to spot money laundering's worst offenders

Kroll's consultants highlight the main signals that something is not right with a bank, and outline what supervisors can do about it.

As forensic investigators of fraud, corruption and money laundering, Kroll's work takes us to fascinating jurisdictions worldwide. It allows us the privilege of working alongside some of the most committed, sophisticated and determined professionals in governments, government agencies, central banks, regulators and financial intelligence units (FIUs) working to identify and prevent such activity.

Money laundering is a global problem – not one confined to a particular market or region. We need to move away from the perception that one market is good and another is bad, and recognise that domestic challenges faced by peers overseas create money laundering risk globally. Then the focus can be on how, working together fluidly through information sharing, these challenges can be surmounted.

Regulators are trying their best, and there is no doubt that banks' financial crime departments are full, in many cases, of well-intentioned employees, and millions are being spent on AML detection systems.

The problem

Money laundering and money launderers operate like some of the most sophisticated, slick and tech-savvy global corporates, with intricately connected global supply chains working closely and without geographical borders.

Yet the global fight against money laundering works in precisely the opposite fashion. There are countries, those countries have regulators, those regulators regulate financial institutions, and those financial institutions review each transaction. If one happens to raise an alert, a suspicious activity report (SAR) may be filed. These SARs are queued up, in often under-resourced FIUs, that must then file requests for information around transactions with other countries, from which they have to wait for a response. All of this takes time, there are multiple stakeholders holding various pieces of the jigsaw, yet no-one is looking at the big picture. Meanwhile, the launderers can move billions of dollars around the world in millions of transactions in minutes, if not seconds.

The authors

Zoë Newman, Regional Managing Director, Emea, and Global Co-head of the Financial Investigations Practice, Kroll
Howard Cooper, Managing Director and Global Co-head of the Financial Investigations Practice, Kroll
David Lewis, Managing Director and Global Head of AML Advisory, Kroll

If we accept that the global AML system is not operating effectively and that it will take some time to fix, what can be done in the short term to identify and stop large-scale abuse of the financial system in order to launder the proceeds of crime?

We could start by identifying and rooting out the worst offenders.

The good, the bad and the ugly

We have worked across developed, developing and emerging markets on behalf of central banks and other regulators, FIUs and financial institutions themselves, helping them to not only identify money laundering risk, but also investigate major systemic issues concerning financial institutions.

Admittedly, our experience is skewed, focused on the worst of the worst, situations that regulators in many western markets would find, at best, far-fetched and, at worst, incomprehensible. But, whether you sit within a developed or a developing economy, none are perfect, and money laundering risk is a common theme throughout.

The question is whether laundering is a by-product of a broader fraud and/or corruption issue that has its provenance in your jurisdiction, or whether you are a transit economy, through which the proceeds are laundered.

Based on this experience, irrespective of jurisdiction, banks fall into one of three categories:

The good

These are banks that are, for the most part, doing the right thing in the prevention and detection of money laundering. They’re not perfect, but are proactive, have a strong governance framework and are doing their best in an imperfect world. The issue is that those that can be described as the standard-setters are few and far between.

The bad

These are the ‘transitory’ banks – those that allow the proceeds of crime to pass through their accounts. To refer to the three stages of money laundering, they perform the layering and integration functions. Broadly they fall into two categories:

- Those that might, at best, be described as inadvertent facilitators of money laundering, either due to framework and governance failures or simply not taking the issue seriously enough.
- The knowing facilitators of money laundering: banks whose primary purpose is to aid and abet wrongdoers in accessing the financial system.

The ugly

The ‘placement’ banks. “Give a man a gun, he can rob a bank; give a man a bank, he can rob a country” is a slightly adapted quote that can best be ascribed to this category. These are banks that are established or acquired with the initial intention or eventual purpose of generating cash for their owners, which can then be laundered and dissipated globally. This might sound extreme but, in our experience, it still occurs with frightening ease. There are a number of common attributes of those markets where this has occurred that heightens the risk profile. These include:

- Jurisdictions deemed at heightened risk due to their geographic location
- Markets prone to a high concentration of power
- A lack of independence or integrity in terms of legal processes
- A lack of independence or autonomy of supervisory functions.

Taking the bad and the ugly, the real point to relay here is that, in every case we have investigated, all the issues were obvious to anyone who looked – hiding in plain sight, if you like. The attributes of money laundering were prevalent internally for many years, and the interrogation of internal data would have highlighted the risks long before the issue grew to such a magnitude that significant intervention was required.

Spotting the warning signs

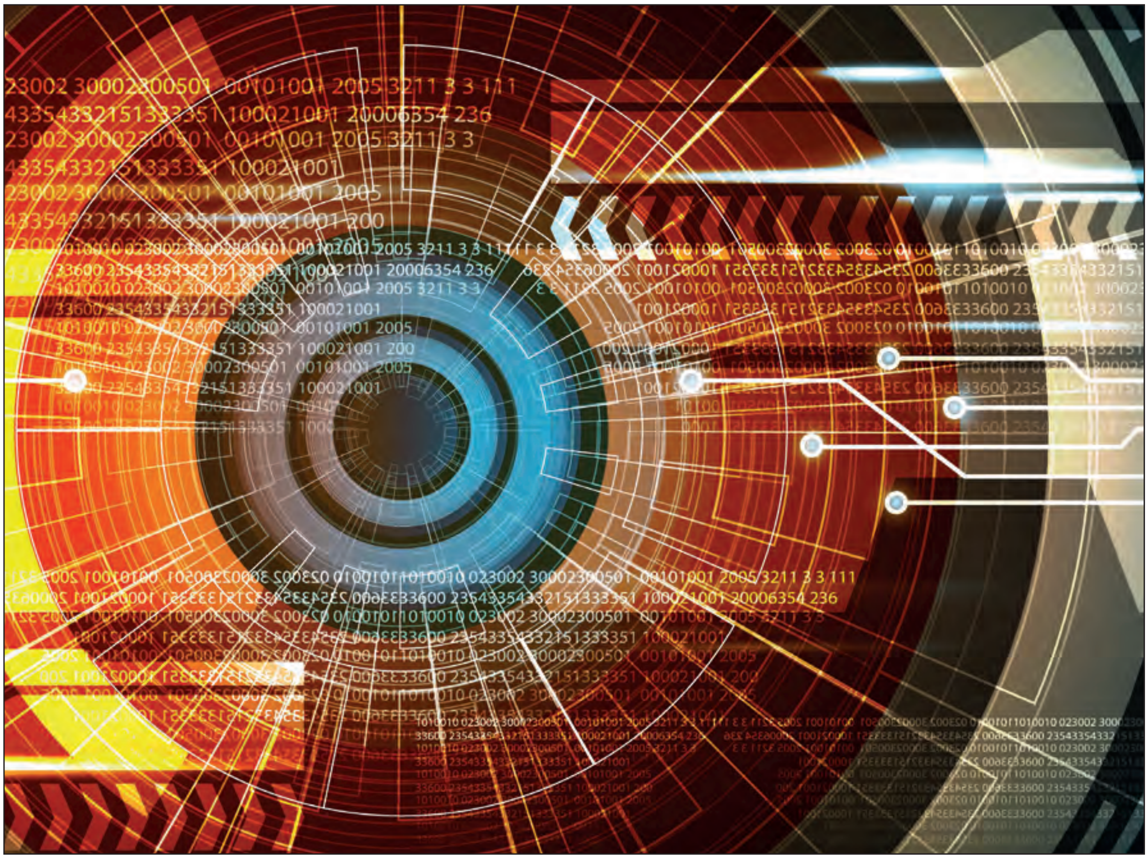
So, if you’re a supervisor, FIU or even investor, what are the warning signs of a bad or ugly bank?

Too good to be true

It is an age-old saying but, if a bank appears as an outlier in its performance, then it’s time to take a look. A common red flag is a rapidly inflating balance sheet, often driven by a ballooning loan portfolio; the balance sheet looks very healthy but, often, what lies beneath is far from the case. These portfolios often comprise significant loans to related parties, both declared and undeclared, and when you start to unpick their provenance, it quickly becomes apparent the majority don’t have sound commerciality behind them. At first glance, all seems sound: a trade-based loan to secure a contract for the purchase of goods by a foreign counterpart. The contractual paperwork is available and the counterparty may even check to a website. However, some brief digging below the surface reveals shell entities, fake websites and nonsensical pricing. Similarly, there may be significant increases in cash deposits, often attracted as a result of interest rates outside of market norms.

Sleight of hand

The dictionary definition of “sleight” is appropriate: “the use of dexterity or cunning, especially so as to deceive.” Although more commonly associated with the techniques used by magicians to divert their audiences, in this context we are talking of the techniques used by bad actors in the banking sector to mislead stakeholders as to the provenance of liquidity or assets within institutions. Loan recycling is the most prevalent here, in that what appear to be new, performing loans are masking years of legacy non-performance by refreshing the borrower when the loan becomes due. It is only when you look at the cashflows within the bank and how they interplay that this becomes apparent.



We have seen similar examples regarding regulator-required capital injections, post-event. On initial analysis of fund flows it is clear this ‘fresh capital’ was actually funded through loans to ‘customers’ of the bank itself, yet it is only through data analytics complemented by practical, investigative research into the viability of counterparts that this becomes apparent.

Finally, we turn to related party transactions – declared rather than undeclared. That needs to be the focus. This can only be identified by taking transactional data, not cross-border but internally, within a bank, to understand which accounts that should be unrelated are actually significantly related, due to the level of their inter-account activity.

Smoke and mirrors

To some readers, in some jurisdictions this will seem far-fetched. But to others it will be a cognisant reality. We refer to those who have successfully gained access to a banking licence, who either deliberately use this to their own advantage or receive benefit from others by providing them access to a financial institution to launder their ill-gotten gains. They can do this by deliberately misleading regulators and the market as to the reality of a situation and, as a result, true exposure is masked. We have also seen smoke and mirrors used regularly in terms of wholesale changes in the ownership of a bank or the customers of a bank. This is often achieved through nominee shareholding structures as well as the use of powers of attorney or trustee agreements.

Lessons learned

If we accept the concept of 'with the benefit of hindsight – everything is obvious', then what can we learn? The real concern is that each of the aforementioned examples relates to real-life situations we have investigated, and that it was obvious, or at least became so, to the regulators or FIUs involved. However, a number of these institutions continued to be audited by firms with well-known brands and succeeded in raising funds on the capital markets. So the real question is: what were the impediments that led to action being delayed until it was too late? There are some all too common themes:

- A lack of resource, particularly in markets that represent the highest risk
- A lack of autonomy on the part of regulators to pursue required remedial actions from domestic forces that might be working against them
- A lack of co-ordination among domestic bodies to inform risk indicators and take actions
- The inability to efficiently and effectively co-operate with international counterparts to obtain strategic intelligence and insight, to inform decision-making and enforcement action.

None of these issues will be news to seasoned supervisors. Indeed, there are some initial signs of progress that move us in the right direction:

- Supervision and oversight need to be designed more around effectiveness than rules. The Financial Action Task Force has been a key proponent of this approach, and its efforts are starting to take effect
- Supervisors are beginning to take an intelligence-led approach to supervision, leveraging the technology and data available to them (such as Swift data and beneficial ownership databases)
- Cross-border collaboration: everyone wants it and agrees it is necessary, but sometimes the impediments seem too hard to surmount. Initiatives are, however, taking the industry in the right direction, perhaps not at the granular level necessary, but progress is being made.

In summary, we need to empower those doing good work on the frontline, in supervisory and intelligence unit roles, to act on the money laundering risks they identify. Treating this as a domestic issue on a jurisdiction-by-jurisdiction basis is only going to further empower the launderers, as opposed to those working within the global fight to prevent it.

Conclusion

It is globally acknowledged by all stakeholders that a lack of co-ordination and international co-operation remains a major hindrance in the fight against money laundering. Yet no single body seems equipped to address it. But what if there was a single source of information that could be analysed and shared by all parties? What if it contained most of the necessary data, was real time, and enabled macro- as well as micro-level analysis to direct supervision and enforcement?

Is Swift not the solution? When this question has been asked before, the response has always been that it wouldn't work or couldn't work. But why not? The current situation in Europe has forced a united response, resulting in the global financial system acting cohesively to identify and stop fund flows relating to certain banks, individuals and entities. Surely that is also possible in normal times, when the fight is less tragic, but just as globally pervasive. ❑

Regulators race to curb crypto asset money laundering

Crypto assets are increasingly used as vehicles for money laundering, but regulating them is not necessarily straightforward. Bernadette Lee reports.

The increasing popularity of crypto assets and the rapid growth of crypto service providers is laying down a challenge to the domestic and global bodies tasked with the fight against money laundering.

Research by the Financial Stability Board (FSB) shows the market capitalisation of crypto assets more than tripled to $2.6 trillion in 2021.[1] Many crypto service providers deliberately position themselves outside the regulatory perimeter, and the FSB highlights how traditional financial institutions are increasingly tangling with the risky assets. As well as posing a threat to stability, crypto assets are proving a convenient vehicle for criminals and terrorists to move funds across borders.

Countries must prohibit or regulate crypto assets through clear rules, says a spokesperson from the Financial Action Task Force (FATF). At the same time, the financial industry needs to understand its obligations and ensure it complies with requirements to curb money laundering and terrorist financing.

Virtual or crypto assets possess many features that make them attractive to individuals and businesses, but they are equally appealing to criminals and terrorists, the FATF spokesperson tells *Central Banking*. These features include their potential for anonymity and transaction speed, and their global reach.

Regulators are also increasingly vigilant to new forms of decentralised finance, including stablecoins. "Risks related to the anonymity of transactions on the blockchain are well known," says a European Banking Authority (EBA) spokesperson. "We are aware that many consortia proposing to develop so-called global stablecoins, by design, are seeking to prevent anonymity."

Stablecoin, a subset of crypto assets, has been gaining traction of late. Stablecoins are backed by a pool of typically low-risk assets such as Treasury securities or fiat currencies. Though they are not subject to the wild swings of bitcoin and other unbacked crypto assets, the lack of regulation and limited disclosures on their operational arrangements have triggered a backlash by regulators. Diem, the Facebook-backed stablecoin project, announced in February this year it would be selling off its assets and winding down, having failed to secure regulatory approval in the US.

Growing interest

That has not dampened the growing consumer and institutional interest in crypto assets and related products and services, including stablecoins. If anything, the Covid-19 pandemic and the recent volatility in crypto asset prices have led to a surge in interest globally. In Turkey, this is made evident by the myriad crypto asset-based payment instruments available in the market and the increase in infrastructures provided by domestic and international players that facilitate the acquisition of crypto assets.

"These initiatives have the potential to undermine confidence in rapidly developing methods and instruments currently used in payments," says a spokesperson from the Central Bank of the Republic of Turkey (CBRT). "In this regard, their use in payments may cause irrecoverable losses for the parties [involved in] the transactions."

Standard-setting bodies including the FSB have been particularly concerned about consumer protection because of crypto assets being used for payment of goods, services and other financial transactions. The CBRT has similar concerns.

"Using crypto assets as 'means of payment' while purchasing goods and services entails significant risks to the relevant parties," the CBRT spokesperson says. "Crypto assets whose values could be excessively volatile are neither subject to regulation or supervision mechanisms nor a central regulatory authority. They have the potential to be used in illegal actions due to their anonymous structures. Their wallets can be stolen or used unlawfully without the authorisation of their holders and the transactions are also irrevocable."

Crypto assets' lack of intrinsic value and their tendency to be subject to price fluctuations have raised further questions about their suitability for consumers and retail investors. Regulators are exploring how the trading process should be regulated, said Eddie Yue, chief executive of the Hong Kong Monetary Authority (HKMA) in a statement released on January 12 this year.

"There is a clear need to promote investor education and enhance product disclosures on this front," he said. "The HKMA and the Securities and Futures Commission of Hong Kong are working together to set out our supervisory expectations on the investor protection aspects of authorised institutions' provision of intermediary services to customers related to crypto assets."

Risks of crypto assets

The interconnectedness of crypto assets and their service providers with the mainstream financial system, which could lead to disruption to the payment and financial system, has prompted regulators worldwide to look into the risks.

The EBA, for instance, as early as January 2019, advised the European Commission (EC) about the need for a common European Union framework for crypto asset activities to address the risks they pose in relation to consumer protection, prudential resilience, operational resilience, and money laundering and terrorist financing. This culminated in the EC's September 2020 proposal for a Regulation on Markets in Crypto-assets, and a July 2021 proposal for a new EU AML/CFT package.

"In terms of money laundering/terrorist financing risks, the EC's July 2021 AML/CFT package is intended to expand the scope of the EU's AML/CFT regime to the full range of crypto asset service providers," says the EBA spokesperson. The package extends the existing EU directive – known as AMLD5 – to custodian wallet providers and crypto-to-fiat exchanges. "The proposal is in line with the FATF recommendations," the spokesperson adds.

The HKMA, concerned about the payment-related activities of stablecoins, has also begun a study on crypto assets and stablecoins with the publication of a discussion paper on January 12. The authority is exploring the possibility of adjusting its existing regulation – the Payment Systems and Stored Value Facilities Ordinance – to ensure payments related to stablecoins are properly regulated in Hong Kong. The HKMA aims to introduce a new regime by 2023/24.

Others are taking an even stronger stance. Reserve Bank of India deputy governor T Rabi Sankar told a conference on February 14 that crypto assets are like Ponzi schemes, "and may even be worse".[2] He said the "very raison d'etre" of crypto assets is to bypass regulations, including AML/CFT rules. "Banning cryptocurrency is perhaps the most advisable choice open to India," he concluded.

Crypto assets and crime

Beyond their use in the retail payment space and other types of financial transactions, the FATF has observed crypto assets being used in a wide range of criminal activities, including money laundering, the sale of controlled substances and other illegal items (such as firearms), fraud, tax evasion, sanctions evasion, computer crimes (including cyber attacks resulting in thefts or ransomware), child exploitation, human trafficking and terrorist financing.

But the value of virtual assets involved in most money laundering and terrorist financing cases detected to date remains relatively small compared with cases using traditional financial services and products, according to the FATF spokesperson. One recent estimate put financial crimes involving crypto at $14 billion in 2021, an all-time high in value terms, but tiny compared with the global financial system.[3]

"Most detected cases involved the use of one type of virtual asset only," the FATF spokesperson says. "Most identified activity relates to offending that is native to virtual assets (for example, hacks, fraud and ransomware payments). However, jurisdictions have identified professional money laundering networks, which use virtual assets as one of their means to launder illicit proceeds and quickly transfer value around the world, for example, converting proceeds of crime from drug sales in cash into virtual assets in order to transfer the profits."

AML controls

Concerns over the potential use of virtual assets for money laundering and terrorist financing led the FATF to revise its standards in June 2019. The amended *Recommendation 15* puts AML/CFT requirements on virtual assets and virtual asset service providers (VASPs). Since then, the global body has been carrying out assessments on jurisdictions in its implementation efforts.

The FATF's second 12-month assessment of jurisdictions' implementation of *Recommendation 15*, conducted in June 2021, showed many countries have made progress but implementation is still far from sufficient. In particular, work remains among FATF-Style Regional Bodies (FSRBs). Most of the less developed countries are members of FSRB. During the June 2021 assessment, the FATF looked at whether countries had taken the necessary action to implement *Recommendation 15*. Its assessments showed that 58 out of 128 jurisdictions have implemented *Recommendation 15*. A total of 74% of FATF members and 33% of members of the FSRBs have passed the necessary laws and regulations to permit or prohibit VASPs.

Among the jurisdictions that have been shown to comply with the FATF recommendations is the Philippines. The country demonstrated compliance with 35 out of 40 FATF recommendations, says Mel Georgie Racela, executive director of the Philippines AML Council secretariat.

"The Philippine authorities are working closely together in accordance with the FATF Recommendations on the adoption of a robust regulatory system and international best practices for crypto assets and stablecoins, as it has always done on matters related to constantly enhancing the country's AML environment," he says. "The Philippines is strongly committed to ensuring that its regulatory frameworks keep pace with the ever-changing AML/CTF landscape."

The full implementation of regulations in jurisdictions is particularly important as the lack of enforcement will lead to jurisdictional arbitrage and an increase in money laundering and terrorist financing risks, the FATF cautioned in a publication released in July 2021.

Up until February 2022, only six countries were rated as largely non-compliant, but none have fully implemented FATF *Recommendation 15*, the FATF spokesperson told *Central Banking*.

Part of the reason for non-compliance is a lack of action on the part of many VASPs in carrying out risk assessments, for example. Further issues include challenges in setting a proper definition for VASPs, the failure to set a customer due diligence threshold specific to virtual asset transactions, a lack of implementation of FATF's 'travel rule' and a lack of guidance for VASPs, according to the FATF spokesperson. "Crypto companies need to take their responsibility seriously and apply AML measures to prevent criminals from misusing their services for illicit financial transactions," adds the spokesperson.

Rapid growth

Perhaps the biggest challenge to jurisdictions complying with FATF's *Recommendation 15* is the rapid growth of the sector. According to the FATF, four years before the revision to *Recommendation 15* there were approximately 265,000 active daily bitcoin addresses. The number doubled to approximately 572,400 in June 2019 when the FATF released *Recommendation 15*. As of April 2021, there were more than 1 million daily active bitcoin addresses. These numbers demonstrate that the revised FATF standards have hardly hindered the growth of the market.

The significant rise in the market capitalisation of virtual assets and their interconnectedness with the mainstream financial system is increasingly prompting regulators worldwide to look into regulating crypto assets and their activities, or impose a complete ban, as seen in countries such as China.

"The virtual asset systems have the potential to revolutionise the delivery of financial services by providing faster and more economical means to transfer funds, both domestic and international, and to further support financial inclusion," says Racela of the Anti-Money Laundering Council (Philippines). "These benefits, however, should be considered along with the attendant risks in virtual assets, considering the higher degree of anonymity involved, the velocity of transactions, volatility of prices and global accessibility." ❑

Notes

1. FSB (February 2022), *Assessment of risks to financial stability from crypto-assets*, https://bit.ly/3LGkzh3
2. T Rabi Sankar (February 2022), *Cryptocurrencies – An assessment*, Keynote address delivered at the Indian Banks Association 17th Annual Banking Technology Conference and Awards, https://bit.ly/3HZrOhQ
3. Chainalysis (January 2022), *Crypto crime trends for 2022: illicit transaction activity reaches all-time high in value, all-time low in share of all cryptocurrency activity*, https://bit.ly/3Juzclu

AML supervision at central banks: 2022 survey

Kroll explores why many central banks are investing in skills and data to tackle money laundering, but resourcing constraints are preventing stronger action, as *Central Banking*'s survey data reveals.

The two years since the outbreak of Covid-19 have been a boon for many criminals. The rise of digital finance – particularly crypto assets – has given them new ways to finance crime, including terrorism, and new channels through which to launder money. Authorities have been distracted, their attention and resources devoted to fighting the pandemic and its economic fallout. Meanwhile, in many countries, generous government support schemes have created even more fertile ground for fraud.

In an interview with *Central Banking*, Marcus Pleyer, president of the Financial Action Task Force (FATF), says online transactions have risen in the past year, and there has been a spate of ransomware attacks where money is laundered through crypto assets (see pages 26–31). IBM's cyber security team reports that ransomware was the most common type of cyber attack in 2021, with a small group of criminal organisations carrying out the bulk of the attacks. Crypto research firm Chainalysis estimates that some $14 billion was sent to illicit crypto addresses in the past year, an all-time high in value terms, but a new low relative to the size of the ballooning crypto market.

Even so, *Central Banking*'s survey data shows traditional institutions such as banks remain a key focus for supervisors and, while international financial flows are the most widely reported risk, large cash payments are not far behind. As Pleyer notes, "cash is still king". Supervisors may be facing new challenges, but the old ones have not gone away.

In the face of a proliferation of threats, what can central banks do? Though they often play a critical role in financial supervision, central banks are only one of many agencies in the fight against money laundering and terrorist financing. *Central Banking*'s survey data suggests many authorities co-ordinate surveillance and enforcement through the financial intelligence units. But law enforcement, government, financial regulators, financial firms and more need to be involved, with further co-operation often needed across borders. It is not a straightforward business to keep these disparate groups working in the same direction.

Technology, while providing criminals with new opportunities, may allow supervisors to gain an edge. Many central banks report using data analytics for AML/CFT purposes, and some are turning to advanced analytical techniques. There is also a growing trend towards risk-based supervision, which means supervisors can devote the most resources to firms with the highest risks, and firms themselves can take a proportionate approach: for instance, setting lower thresholds of due diligence for the poorest members of society.

The survey highlights that, while there is a broad push among central banks to improve oversight, there is still a lot of work to do. A significant minority of respondents report not using data analysis to assess AML/CFT threats. Some have seen resourcing levels fall and many more report that resourcing is flat, a challenge that could become worse as governments look to repair their finances after the shocks of the Covid-19 pandemic. Data quality issues and limits to cross-border co-operation add further hurdles.

Central banks will need to be innovative in the coming years to make targeted interventions and make the most of their limited resources. Technology demands specialist skills, which come at a price. Yet automation and artificial intelligence (AI) also hold the promise of cost savings and new insights, so investment now could pay dividends for years to come.

Data and methodology

Central Banking conducted the AML/CFT survey in January and early February 2022 and received responses from 21 central banks. There were five responses from Africa, six from the Americas, three from Asia-Pacific (including the Middle East) and seven from Europe. Of these, 16 are classed as emerging and developing economies by the International Monetary Fund (IMF), and the other five are advanced economies. Respondents shared data on condition of anonymity.

Key findings

- AML teams are typically fairly small. Central banks with a dedicated team report a median size of 18 staff members.
- The focus remains on traditional financial institutions – 81% say they oversee banks, but only 19% oversee crypto firms and 14% fintech firms more broadly.
- Few financial firms seem to lose their licences because of AML breaches. Only 24% of respondents have rescinded at least one licence in the past three years.
- Cross-border financial flows are seen as the number one source of risk, with 76% of respondents warning this is a key concern.
- More than half of respondents say a lack of resources is hampering their AML efforts.
- On- and off-site inspections remain key tools for supervisors looking to address money laundering risks.
- Two-thirds of respondents report using data analytics for AML purposes. Of these, 71% say they use forms of automated data collection.
- There are many hurdles to better use of data. The wide range in the size and complexity of supervised entities is a concern (67% of respondents), followed by a lack of technical tools (62%).
- Collaboration, including data sharing, is common on a domestic level. But authorities are much less likely to collaborate and proactively share data with global counterparts.

The median 2020 GDP of respondents was around $38 billion, and median GDP per capita was $12,000, based on IMF figures. The smallest central bank had fewer than 200 staff and the largest more than 5,000, with a median of roughly 600, according to data from the *Central Banking Directory*. As a share of total staff, the proportion of staff devoted to AML/CFT functions ranged from 0–16%, with a median of 2%.

Respondents face significant differences in the scale of local oversight challenges. Some report overseeing as few as 23 institutions, but others are responsible for more than 3,000. The median number of institutions being overseen was 109.

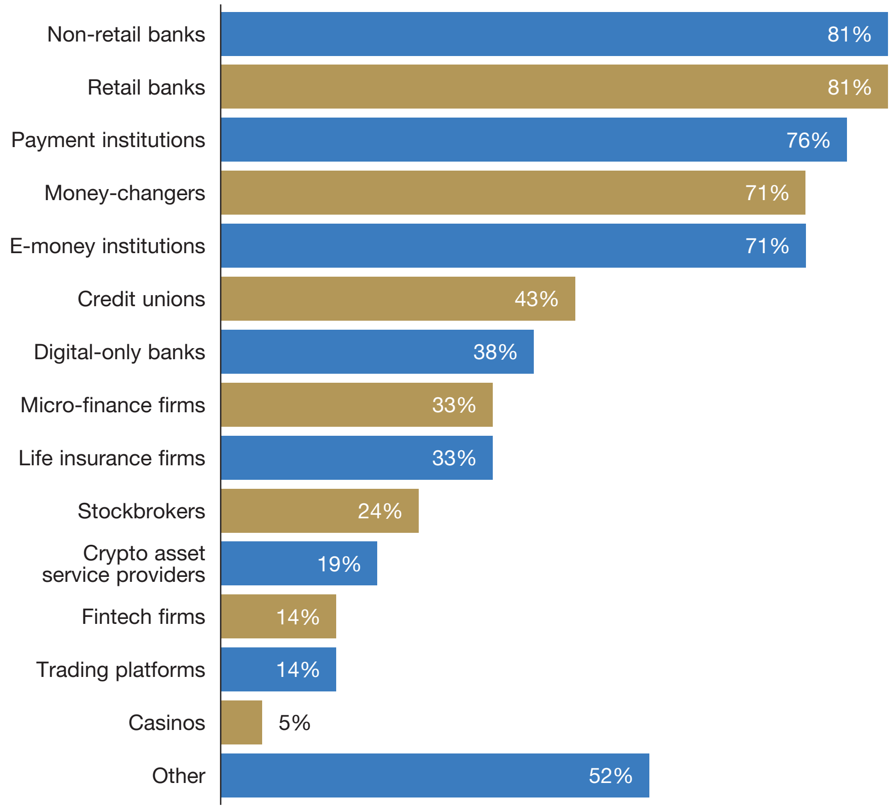
Governance and staffing

The vast majority of respondents (80%) reported having a specific department devoted to AML/CFT. These central banks reported having a team size ranging from four people (on a full-time equivalent basis) to as many as 56, with a median value of 18.

The handful of central banks that do not have a specific AML function typically reported that they have some staff in the wider central bank devoted to AML, though this tends to be a smaller number than those with a dedicated function. AML staff numbers at these central banks ranged from 0–13, with a median of six.

A central bank in the Americas mentioned it had recently established an "AML outreach unit", which is tasked with its external engagement. The unit works with industry, attends research conferences and produces publications to communicate supervisory and regulatory developments.

1. Which institutions fall within your AML framework?



Another institution, based in Europe, said it established a standalone directorate devoted to AML/CFT and consumer protection in 2019. The directorate reports directly to the governor. Similarly, a central bank in Africa said it established a new AML section in 2019 and completed its recruitment process for the team in 2021. This central bank is implementing a risk-based supervision framework with technical assistance from the World Bank.

The high proportion of respondents with a dedicated AML department may reflect a degree of self-selection. Some central banks that declined to participate in the survey cited the lack of an AML department as their reason. *Central Banking* did not approach financial regulators or other AML authorities.

Scope of oversight

More traditional financial firms remain a key focus for most central bank supervisors. A total of 81% of respondents said they oversee retail and non-retail banks for AML risks, and 76% oversee payment systems (see figure 1).

Newer players such as crypto firms are still only subject to oversight in a handful of jurisdictions – 19% reported overseeing crypto asset service providers and only 14% oversee fintech firms more broadly.

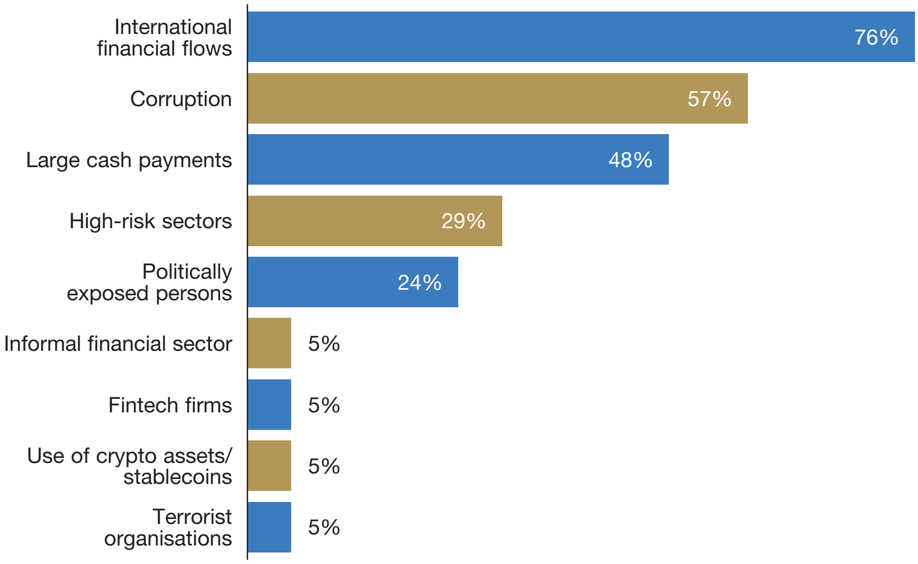
Central banks that chose ‘other’ as an option reported supervising institutions, including informal money lenders, trust companies, remittance providers, housing finance and insurance intermediaries.

Only five respondents reported that they had rescinded a firm’s licence in the past three years (24% of the sample). These five central banks tended to be from wealthier jurisdictions (with an average GDP of $180 billion, versus $110 billion in the sample as a whole). They also tended to have more staff devoted to AML than the average (25 versus 18 in the whole sample).

Risk factors

Comfortably the number one risk factor was international financial flows, reported as a key concern by 76% of respondents. Corruption came in at number two (57%), followed by large cash payments (48%) (see figure 2).

2. What are the most significant risk factors in your jurisdiction?



Echoing figure 1, the data shows that central banks still view newer threats, such as crypto assets and fintech, as lesser concerns. Only 5% reported crypto and fintech as major risk factors in their jurisdictions.

This may be starting to change. The Financial Stability Board's (FSB's) latest report into crypto assets noted crypto markets were on a path to becoming systemically important. But they are not there yet.[1]

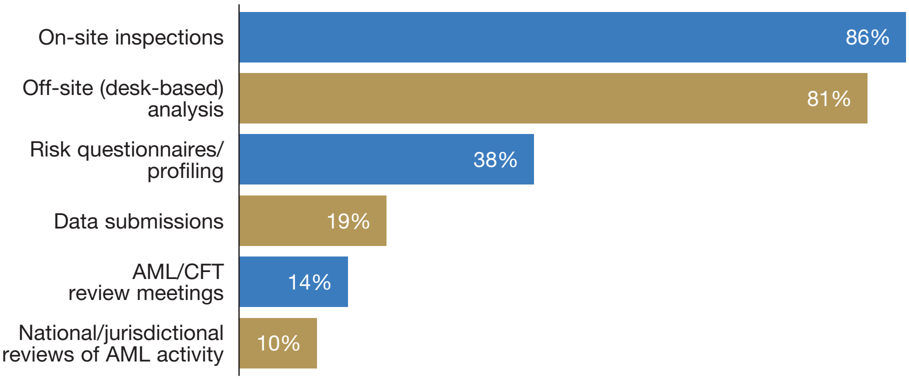
Supervision: tools and challenges

Despite the impact of Covid-19, the most commonly reported supervisory tool was on-site inspections of financial firms, in use at 86% of respondents. A further 81% reported off-site, desk-based reviews as a key tool. The latter has grown in importance since the advent of social distancing rules, but it remains to be seen whether the balance between on-site and off-site reviews has permanently shifted.

Central banks reported having conducted anything from just one supervisory inspection in the past year to as many as 463, with a median of 12 inspections (see figure 3).

Many central banks commented that they used risk-based approaches to supervising money laundering/terrorist financing risks, as advocated by the FATF. One advanced economy central bank in the Asia-Pacific region said it employed risk-based supervision. This central bank said it had moved away from "fixed on-site inspection cycles" towards "more dynamic and timely" interventions. The respondent highlighted three key tools: use of data analytics to identify high-risk activities; supervisory interventions to "dynamically disrupt" high-risk activities; and targeted inspections to direct remediation at high-risk firms.

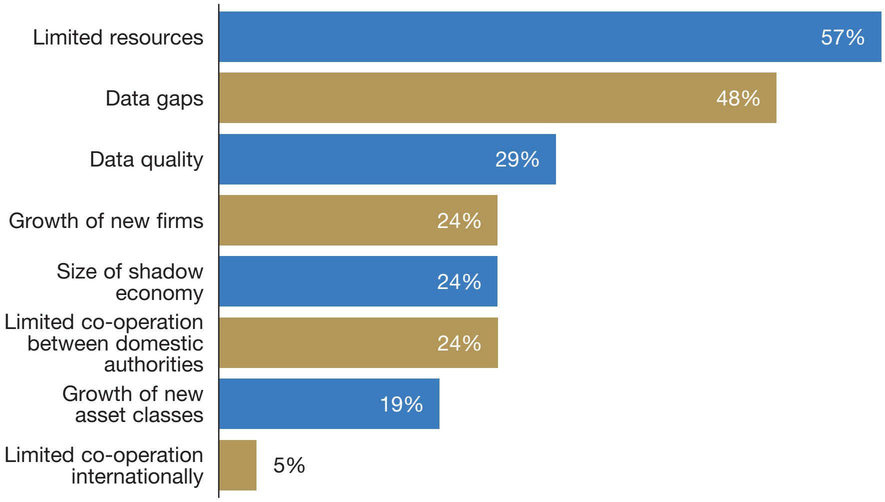
3. Which methods does your central bank consider most important when supervising entities for AML/CFT risks?



A second central bank in Asia-Pacific stressed the importance of its AML risk rating system, which allows supervisors to make systematic assessments of firms' risk profiles. This feeds into the wider process of risk-based supervision. To further support these efforts, the institution carries out periodic sectoral risk assessments.

Risk-based supervision could help central banks meet other objectives as well. A central bank in the Americas commented that it had implemented a simplified due diligence approach to allow banks to set up accounts for vulnerable people in society, "including low-income and undocumented persons".

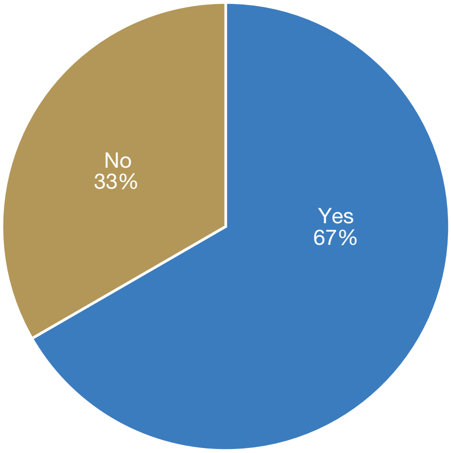
4. What are the main obstacles to improving AML/CFT oversight in your jurisdiction?



Many respondents said they employed regular reviews of AML risks across their whole jurisdiction. Central banks reported their most recent review fell in years ranging from 2013–22. The most common response was 2019.

Central banks face an array of challenges when it comes to improving their AML supervision. Over half (57%) said limited resources was a major obstacle. The second most important was data gaps, reported by 48% of respondents, followed by data quality, at 29% (see figure 4).

5. Do you use data analytics to identify AML/CFT risks?

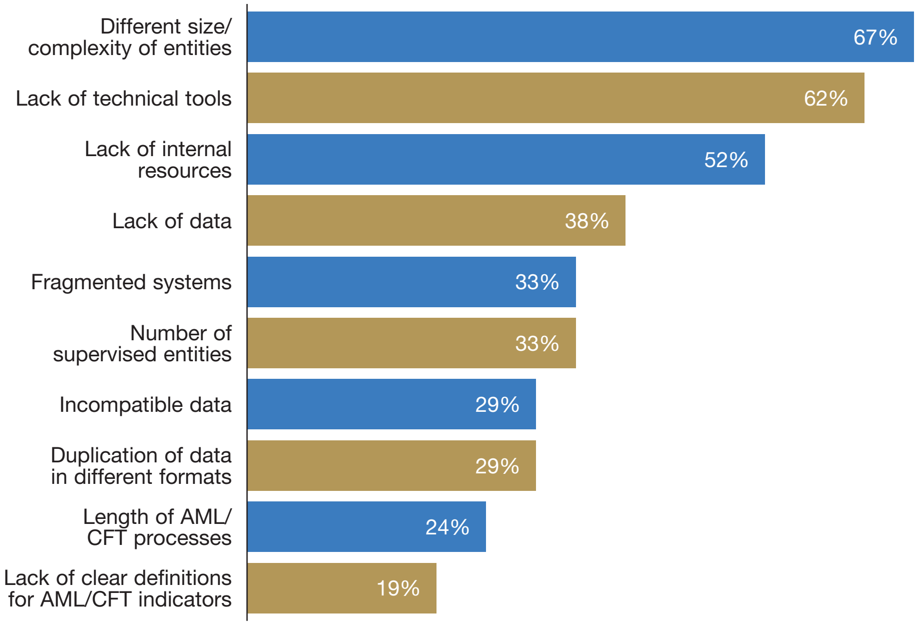


Data: analytics and obstacles

Exactly two-thirds of respondents said they use data analytics to help them identify AML risks. Of these, the most commonly reported data tool was the use of automated data collection (in use at 71% of respondents that apply data analytics). The use of data in external public records was also common, at 64% of respondents. Much less used was AI or machine learning, in use at just one central bank. Big data or 'alternative' data was used by three (21%).

The figures show a significant minority of central banks in the sample (33%) do not use data analytics in their AML work, suggesting this could be an area of expansion in future years (see figure 5).

6. What are the greatest challenges your central bank faces when gathering AML/CFT data?



However, for data use to become more widespread and effective, central banks will have to overcome a range of obstacles. The most commonly reported problem was the sheer range of institutions on which data must be gathered, given their differing size and complexity – 67% of central banks said this was a problem. A further 62% said a lack of technical tools was holding them back, while 52% mentioned a lack of resources (see figure 6).

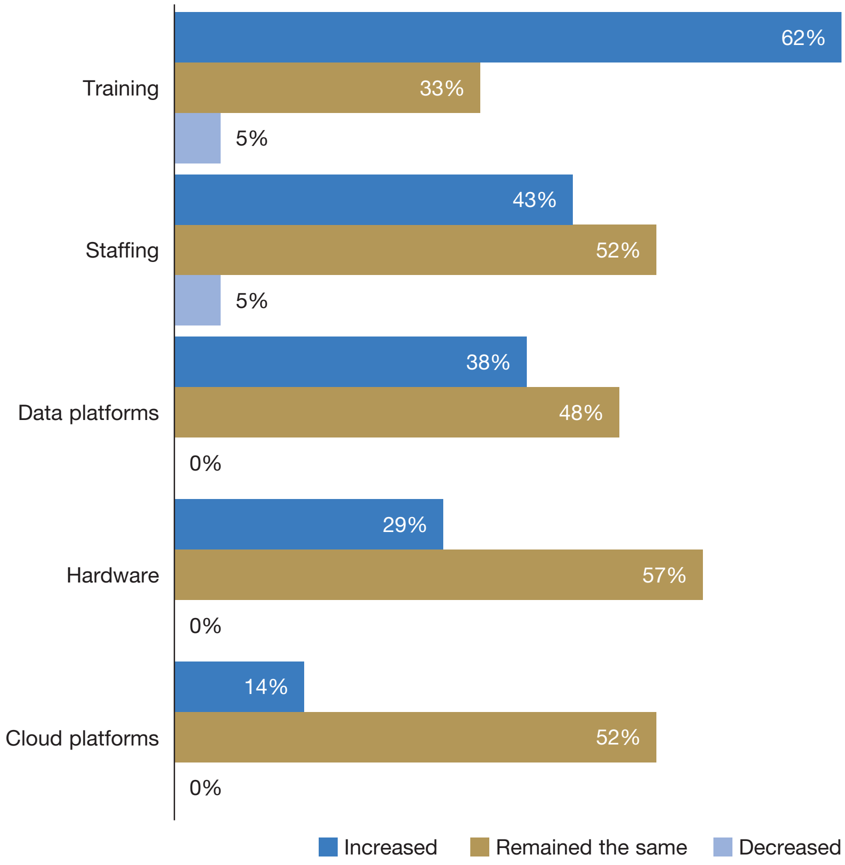
At the other end of the spectrum, AML definitions (19%), lengthy processes (24%) and data duplication or incompatibility (both 29%) were less commonly reported as challenges.

Resourcing

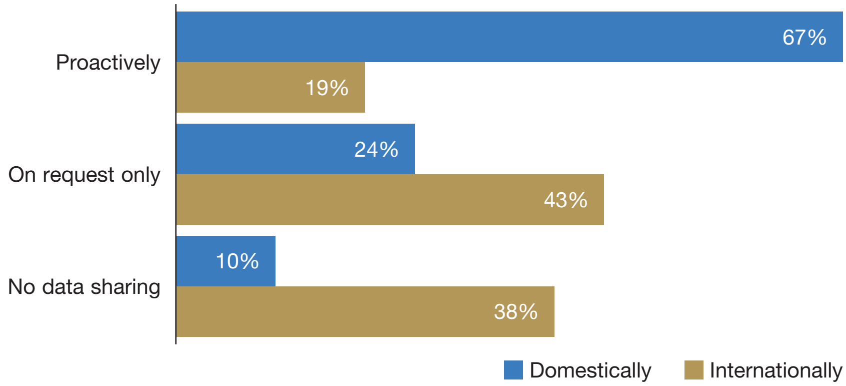
The broad trend appears to be towards either greater resourcing of AML functions, particularly in the staff and training categories, or constant levels of resourcing. One central bank reported that its staffing resource had fallen in 2021, and one other reported that its training resources had fallen (see figure 7).

Somewhat less seems to be invested in data platforms, hardware – for instance for data processing – and cloud platforms. Only 14 central banks commented on cloud resourcing, which may indicate that use of the cloud is still relatively limited, at least for AML purposes.

7. In 2021, did your central bank increase or decrease AML/CFT supervision resourcing in the following areas?



8. Does your central bank share data relating to suspicious activity with other authorities?



Given that central banks report a lack of resources as a key concern, more investment in AML may be needed. One central bank in Africa commented that recent reforms to the AML function had led to greater co-operation with local and overseas authorities, which had the additional advantage of allowing pooling of resources.

Collaboration and data sharing

The data suggests authorities have closer ties to domestic authorities than to their counterparts abroad, which could hamper efforts to improve information and data sharing. Since central banks report international financial flows are a key concern, strengthening global ties seems an important priority.

It is common to have a body tasked with co-ordinating AML/CFT authorities domestically. Only four central banks (19%) said they did not have such a body in their jurisdiction. Most of those that have a body mention that this is either the country's financial intelligence unit or a council specifically formed to co-ordinate AML matters.

Similarly, most central banks report that they share data on suspicious activity domestically. Two-thirds say they share data on a proactive basis, and another 23% say they provide data on request. Only 10% say they do not share data at all domestically (see figure 8).

A central bank in the Americas reports it is undertaking a project to centralise know-your-customer data at a national level. Financial institutions and regulators will be able to access the data. The project is expected to enter production in July 2022.

All respondents say they are engaged with some form of international collaboration on AML. Regional groupings are the most common (76%), followed by bilateral co-operation (67%) and international bodies (48%).

However, many central banks (38%) do not share any data on suspicious transactions internationally. A further 43% said they share data on request, while only 19% of central banks share data proactively on an international level. ❑

Notes

[1] FSB (February 2022), *Assessment of risks to financial stability from crypto-assets*, https://bit.ly/3LGkzh3

Collaboration is key: how central banks are tackling money laundering

Kroll explores *Central Banking*'s survey data on how central banks are fighting money laundering. Many will need to step up their work with data and risk-based supervision to cope with new threats.

KROLL

Introduction

In collaboration with *Central Banking*, Kroll conducted a survey of central banks across Europe, Africa, the Americas and Asia-Pacific with questions focused on AML/CFT supervision. Unsurprisingly, the majority of respondents comprised those that have AML/CFT supervisory authority over regulated entities, specifically retail and non-retail banks, with other countries designating this authority to standalone supervisors or a hybrid financial intelligence unit (FIU). The respondents to the survey were largely based in emerging market economies; however, when it comes to AML/CFT supervision, the perception of risks – as well as supervisory models adopted by central banks – are mostly consistent, regardless of geographic location and the size of the economy.

The survey results reveal that central banks face significant risks from cross-border payments, and their supervisory models are under strain as the payments landscape changes with the rise of payment and e-money firms. Although there is an emphasis on on-site inspections, the rise in the use of data analytics and the adoption of risk-based supervision models is enabling central banks to overcome resourcing challenges and better manage risk. Finally, AML/CFT supervisors are improving their ability to co-operate domestically, but there is significant room for improvement in international collaboration to effectively combat shared financial crime risks.

AML/ CFT risks

Central banks reported three common AML/CFT risk factors: money laundering methodologies utilising cross-border fund flows, large cash deposits and the laundering of the proceeds of corruption. It is evident from the survey responses that central banks can do more together to manage and respond to these risks.

The authors

Zoë Newman, Regional Managing Director, Emea, and Global Co-head of the Financial Investigations Practice, Kroll
Howard Cooper, Managing Director and Global Co-head of the Financial Investigations Practice, Kroll
David Lewis, Managing Director and Global Head of AML Advisory, Kroll

Cross-border fund flows: a consistent risk

Money laundering involving international financial flows is the most common concern for supervisors, with 80% of respondents considering it to be one of the most significant AML/CFT risks. There is potentially, however, a significant gap in the ability of supervisors to respond to the risks these cross-border payments present.

More than one-third of respondents reported that they do not proactively share data on suspicious activity with international partners. In fact, less than half share information even upon request from international partners, with only 19% proactively sharing relevant data.

Kroll has significant experience investigating complex cross-border money laundering schemes. The defining feature of all of these schemes, regardless of how the illicit funds were generated or the countries involved, is the co-ordinated movement of illicit funds through multiple jurisdictions. The schemes all exploited visibility gaps across jurisdictions as the funds went through the placement, layering and integration phases of the money laundering cycle. We have seen first-hand the success that can be achieved through supervisory agencies sharing relevant data across borders to detect, analyse and investigate financial crime schemes.

The majority of central banks do, of course, report information on suspicious activity to their FIU, which may in turn share information with their international partners. Supervisors are often the first to identify high-risk, unusual and suspicious activity, and high-level findings or details of specific transactions may be shared with their FIU counterparts. Systemic issues discovered within one regulated entity are often not used to assess the risk of non-reporting to the FIU and how the identified failings may have had a contagion effect across the economy. Crucially, reports on high-risk entities fail to be disseminated to foreign AML/CFT supervisors to assist them in assessing and mitigating risks in cross-border fund flows.

Cash is still seen as king

Many central banks still see cash as king when it comes to money laundering methodologies. Despite the ever-increasing use of electronic payments and corresponding reduction in the use of cash in many economies, more than half of respondents consider large cash payments to be a significant AML/CFT risk.

Cash remains the primary means of value transfer in illicit activity such as the drug trade and untaxed shadow economy; however, in Kroll’s experience investigating large-scale international money laundering, the use of physical cash is negligible.

Regulated entities do, of course, need to monitor and be alert to the use of illicit cash entering the financial system. It is, however, arguable that the continuing focus on cash and the relative simplicity of transaction monitoring systems to detect cash deposits means resources are not allocated to detecting more complex typologies using cross-border payments. This in turn causes an overreporting of cash-based suspicious transaction reports that impact on risk perceptions by supervisors.

Corruption and politically exposed persons (PEPs)

More than half of respondents (57%) reported illicit funds from corruption to be a significant AML/CFT risk. This contrasts with only 23% of central banks that consider PEPs a significant risk. In almost all cases, corruption schemes involve a PEP, their family or close associates, and the survey results may represent evidence of a disconnect in the understanding of AML/CFT risks stemming from corruption.

We have seen many cases where illicit funds linked to corruption have been moved through and, ultimately, deposited in foreign jurisdictions for the benefit of PEPs. In some cases, the regulated entities that ultimately received the funds had identified the ultimate beneficial owner as a PEP but had not adequately assessed the AML/CFT risks of the funds they were receiving. Related to this is a focus by supervisors on monitoring how effective regulated entities' know-your-customer (KYC) programmes are in identifying PEPs, rather than assessing the risks of the money movements through their accounts.

Supervisory scope

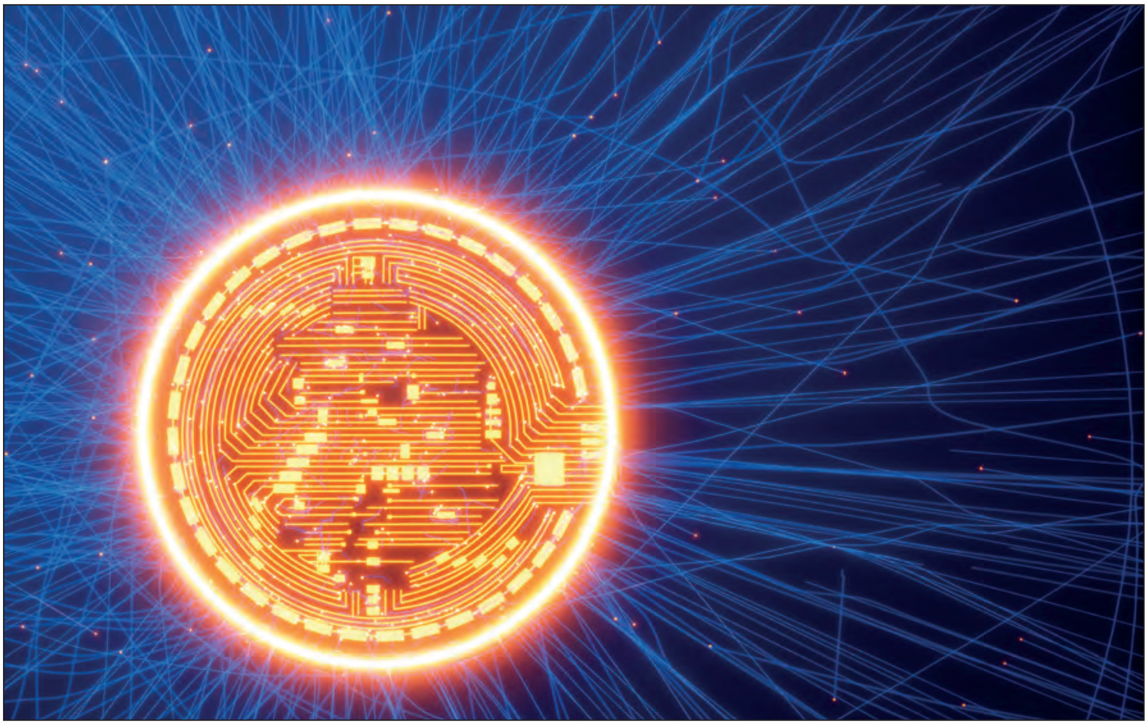
In many ways, AML/CFT risks faced by central banks have remained the same over the years. But there has been a rapid change in the types of regulated entities operating in the financial system and the types of services they offer. Central banks are facing challenges to maintain effective oversight in this expanded ecosystem.

Banks remain the focus, but other institutions are on the rise

Unsurprisingly, the majority of central banks that exercise AML/CFT supervisory powers retain oversight of retail and commercial banks, reflecting the primary role these institutions maintain in the financial system. However, it is clear that the operating environment is changing, and recent years have seen an explosion in the number of payment services and e-money companies challenging banks for market share in transaction services. These include payment processing companies servicing online and physical businesses and online money transfer companies. This shift has seen a rebalance where AML/CFT risks – particularly when it comes to cross-border payments – lie across the spectrum of regulated entities.

Reflecting this, 75% and 80% of respondents have supervisory responsibility for e-money institutions and payment firms, respectively; market operators are commonly classified as fintech companies. The challenge remains for central banks to adapt their supervision models to deal with this seismic shift in the transaction landscape and the number of regulated entities, to effectively manage risks.

The survey revealed that only 15% of respondents consider fintech firms to represent one of their most significant AML/CFT risks. There is a danger that central banks view these firms as simply providing traditional bank services, for example cross-border payments, in a new way. This could lead to a failure to adapt their supervision model to reflect the vastly different operating models between these new entrants and traditional banks.



Cryptocurrency firms often occupy a legal grey area and remain unregulated in some advanced and emerging economies

Crypto: an emerging risk?

Cryptocurrencies and virtual assets have evolved over the past 15 years – from a niche industry to one enjoying significant public attention and wider adoption among traditional financial market participants. There has been corresponding attention paid by governments and the wider public to the AML/CFT risks present in the industry. Where not banned outright, cryptocurrency firms often sit within a legal grey area and remain unregulated in a large number of advanced and emerging economies. The small number of central banks (19%) in our survey that have AML/CFT supervisory responsibility for the cryptocurrency sector may reflect this patchwork legality and regulatory oversight of the industry.

Equally, despite the high profile that cryptocurrencies and virtual assets currently enjoy in the public's mind and the perceived legal and regulatory focus on the industries in recent years, only one respondent considered cryptocurrencies to present a significant AML/CFT risk.

Regardless of views on the size of the AML/CFT risk posed by cryptocurrencies and virtual assets, central banks need to be aware of the existence and operations of these firms within their jurisdiction to ensure there is effective AML/CFT oversight and that other regulated firms are adopting appropriate controls when interacting with cryptocurrency firms.

Nature of supervision

With the number of regulated firms and the complexity of their operations and service offerings undergoing a rapid change, central banks are facing a distinct challenge to adopt their supervisory models to adequately manage and respond to AML/CFT risks. The increasing number of those adopting dynamic approaches in line with international guidance and best practice are reporting fewer challenges and improved outcomes.

Traditional scheduled inspections remain the norm

The main supervisory tool for central banks is the traditional on-site inspection with all relevant central banks using these to assess AML/CFT risks and compliance within regulated entities. Almost all central banks (85%) combined on-site inspections with off-site desk-based analysis.

A number of supervisors (40%) are utilising risk questionnaires to assist with profiling prior to an on-site inspection, but only 20% are utilising data gathering and analysis before the inspection process.

As outlined, most jurisdictions are seeing a huge rise in the number of regulated entities and the complexity of services offered by these firms. There is a real danger of central banks being unable to effectively oversee regulated firms if they continue to rely on a system involving regular on- and off-site inspections of all regulated entities. This is compounded by the resource constraints under which many central banks are operating.

Despite exercising wide-ranging AML/CFT supervisory powers, two respondents did not have a dedicated AML/CFT department within their central bank. Average staff allocated to AML/CFT oversight was just six in these two central banks, compared with an average of 20 among respondents with a dedicated AML/CFT department. In addition, more than half of respondents reported facing resourcing limitations that negatively affect their ability to exercise their supervisory powers.

Countries are adopting dynamic approaches to risk management

In a positive development, a number of countries have adapted, or are in the process of adapting, their supervisory approach in line with the Financial Action Task Force's (FATF's) *Guidance on risk-based supervision*, issued in March 2021. Namely, this is the adoption of a dynamic supervisory approach harnessing data analytics to proactively detect higher-risk activity and firms. Supervisors can then apply their interventions in a more timely and targeted way to address these risks.

Central banks that have adopted a risk-based supervisory approach all report an improvement in their ability to develop a more holistic and current understanding of AML/CFT risks and to devote their scarce resources to targeting those entities and activities that present the highest risk. This ability to adapt has revealed itself to be even more important since the Covid-19 pandemic began, with many central banks reporting they have been unable to conduct on-site inspections.

The survey results suggest that the adoption of a risk-based supervisory approach appears to be correlated with a country undergoing the FATF mutual evaluation process, and we foresee that many more countries will adopt this approach as they prepare for and go through the mutual evaluation cycle. A number of countries that are preparing to or are currently undergoing a mutual evaluation also reported an increase over the past 12 months in staff, software and training.

More countries are using data analysis to detect AML/CFT risks

There is an increasing focus among respondents on using data analytics to detect and monitor AML/CFT risks with two-thirds of central banks currently using data analytics in their work. Of these, the majority rely upon the automated collection of data from supervised entities, with a smaller number making use of external public records and exchanges of data across borders.

A significant challenge faced by most central banks when using data analytics is the different size and complexity of operations of supervised entities. This is compounded by the duplication of data or incompatibility of data for analysis across the supervised entities. In addition, central banks report a lack of the required technical tools and skilled staff to conduct this work.

Although only 20% of respondents reported collecting data submissions from regulated entities to assist with their work, in Kroll's experience, central banks often possess or have access to a huge amount of data that, if utilised in the correct way, can be a tremendous resource in assessing AML/CFT risks and exercising supervisory powers. For example, high-level cross-border payment data can often provide indicators of unusual or suspicious transaction activity, which can allow supervisors to target specific regulated entities.

Emerging trends

Greater collaboration with domestic agencies and public-private partnerships

In contrast with international engagement, and encouragingly, two-thirds of respondents share relevant data proactively with domestic agencies. In line with international best practices, a number of jurisdictions reported the recent establishment or expansion of domestic co-ordination bodies or forums, including relevant authorities with AML/CFT responsibilities (for example, FIUs, other AML/CFT supervisors, regulators, police and prosecutors). These collaborations are seen as a critical element in successfully developing robust AML/CFT policies and legal frameworks, as well as the enforcement of existing laws.

One-quarter of respondents still report that a lack of co-ordination among domestic agencies impacts their ability to effectively oversee and manage AML/CFT risks in their jurisdiction. In many instances, a country's laws and regulations are not a barrier to domestic co-operation. The challenge often faced is to develop a cohesive strategy with shared goals and desired operational outcomes that benefit all participants.

Similarly, a number of jurisdictions have developed public-private partnerships, providing a forum for government, regulated entities and other interested parties to share intelligence and knowledge on AML/CFT matters. These partnerships also extend to the development of shared KYC and transaction monitoring tools, allowing regulated entities and government agencies to have insight into relevant data to assist in their respective compliance, investigative and supervisory capacities.

These shared technology solutions are without doubt a positive step in the fight against financial crime. With many countries adopting different models, supervisors need to collaborate to ensure lessons from the development of each of their tools is being shared and to ensure there is some consistency across borders.

The future

Central banks are operating in an ever-evolving and complex environment, and this will surely continue. The growth of fintech firms and new payment methods will present challenges in their ability to assess and manage AML/CFT risks – particularly in regard to cross-border fund flows. Countries can and should be working to adopt more dynamic risk-based approaches to supervision, harnessing data analytics to utilise their scarce resources more effectively.

Collaboration is the key component in the fight against financial crime, and countries should continue to work with their domestic partners, while more proactively developing relationships to share intelligence with foreign partners to combat the shared money laundering risks all countries face. ❑

How supervisors can step up the AML fight

Marcus Pleyer, president of the Financial Action Task Force, says digital tools, stronger co-operation and risk-based methods can give supervisors an edge. But threats are still proliferating, he tells Daniel Hinge.

What has changed in the fight against money laundering since you took office as president of the Financial Action Task Force (FATF), in July 2020?
Marcus Pleyer: My presidential term has been very much impacted by the Covid-19 pandemic, so what we see is of course an increase in fraud, including that in relation to government aid. We see a surge in online transactions – that is a high priority for us currently. Also cyber security issues, such as ransomware attacks where the money is laundered through crypto.

Virtual assets have expanded over the years, and are now really increasing. At the beginning, if you compared virtual asset transactions to real money transactions, the gap was huge – it's still huge but it is diminishing. Virtual assets are creating opportunities for criminals and, without regulation, they could become a safe haven for financial transactions with links to crime or terrorism. This is why it is very important our new rules on virtual assets are effectively implemented.

These one and a half years also saw a huge discussion about stablecoins. We have all observed the decline of Libra or Diem, but I think the discussion will not go away, and neither will the phenomenon. This is something that is much more attractive for normal consumers, so it is something we have to look at. Central banks also have to look at whether they want to work on their own digital currencies.

There is also the whole area of decentralised finance, which tries to promise total anonymity and no centralised control. That is, of course, a challenge. Ultimately, however, if a business provides financial services, then it needs to apply AML rules.

One of your aims has been to drive digital transformation in AML and CFT. What are some of the key goals here, and how is that work progressing?
Marcus Pleyer: The FATF has for a long time looked to the risks of digital transformation. But I think we should also look at the opportunities the technology offers for the fight against money laundering.

I am very aware that we see high numbers of suspicious transaction reports (STRs), but they do not correspond with the extremely low numbers for convictions. There is a gap, and digital tools can make the fight more efficient on the side of the private sector, through know-your-customer checks, monitoring and STRs, but also for the operational agencies such as financial intelligence units and law enforcement agencies.

Marcus Pleyer became president of the Financial Action Task Force (FATF) on July 1, 2020, having previously held the position of vice-president for two years. He also currently serves as deputy director general in the German finance ministry, where he is responsible for policy development and international engagement on global financial markets, as well as AML, digital finance and more. Pleyer holds a master of law degree from the University of Edinburgh, a master of business administration from the University of Wales and a PhD from the University of Dresden. He also studied law at the National University of Singapore and University of Heidelberg before qualifying as a judge in 1997.

Under my presidency, we began a series of projects on how supervisors, operational agencies and the private sector can harness the opportunities of new technologies. We also highlight examples of best practices in how to overcome the challenges when incorporating these new technologies into your AML workflows.

We see money laundering and terrorist financing cases taking place across financial institutions, across borders and in a speedy manner. On the other side, the AML/CFT authorities need to strengthen their capacity to respond to these threats and also be fast and work with high-quality, efficient measures.

Digital tools can also help with a more granular application of a risk-based approach. This can open up room for financial inclusion, bringing more people into the regulated financial system. By doing that, you also improve the effectiveness of AML/CFT measures.

Our aim is to identify the opportunities of digitalisation, such as digital ID. The FATF has been the first international organisation to publish and advise on digital ID. It came just in time – in spring 2020 when the banks were unsure how to proceed, especially with identification.

We also identify the necessary conditions, policies and practices that need to be in place to successfully implement these technologies. Finally, it is important the public sector better understands how digital technology can help detect and investigate money laundering, and how the private sector uses these technologies.

Would you say authorities are gathering enough data for AML purposes?

Marcus Pleyer: Instead of focusing on whether they collect sufficient data, I would focus on whether such collection is risk-based. The data needs to be focused, targeted and proportional. It needs to help countries respond to the most important risks, to identify the emerging trends. Data collection needs to be tailored to address national AML strategies and priorities.

Having risk-based data collection can also minimise potential data privacy concerns and better respect the rights of individuals. This is something that is important to me, and the FATF has started a project on how digital tools can help information sharing while protecting the data.

In the past two years, we have been looking at the level of digital adoption of our members. More and more countries have been adopting digital solutions, especially to support data collection, data triage and analysis processes. But collecting more data is different to collecting the right kind of usable data. What we see is countries sometimes spending a lot of effort on data cleaning before they can use the data in a meaningful way.

You mentioned the importance of a risk-based approach. Is this method becoming more common among FATF members?
Marcus Pleyer: It is, definitely. We introduced the risk-based approach eight or nine years ago. It is a long process and countries need to move away from a tick-box approach to a more risk-based focus.

Risk-based is, in a way, a kind of proportionality: you have to tailor your measures in a proportional way. You must be effective, but you don't have to exaggerate. We don't want firms to de-risk and terminate all of their clients, we want a really tailored approach where institutions concentrate on individual risks.

What digital tools might authorities consider adopting?
Marcus Pleyer: To be clear, the FATF does not prescribe particular tools but, in our project on the opportunities of new technology, we highlight how different types of digital technology – from advanced analytics to machine learning – can have the best potential to improve the efficiency and effectiveness of AML/CFT measures. For example, machine learning reduces the need for manual input into monitoring, it reduces false positives and it helps identify complex cases. Artificial intelligence (AI) can detect patterns of suspicious transactions much more easily than the human brain. Then there is natural language processing (NLP) and soft computing techniques that are useful for analysing a vast amount of data from disparate sources, such as the text in STRs.

Again, we are not concentrating on particular companies or fintechs, but highlighting what the technology can offer. FATF is a great platform for information exchange. You may know that our members and regional bodies equate to more than 200 countries. So, if there are great solutions in one or two parts of the world, they can easily be exchanged globally. It's a wonderful knowledge platform.

Are you seeing greater use of innovative forms of data, more use of unstructured data, text data, and so on?
Marcus Pleyer: If a financial intelligence unit receives millions of STRs a year, NLP can help categorise and analyse the information.

There is much more data to explore, not only payment information but also companies that bring in new data. When you identify your customer, this is not only about scanning their passport, you can also find out if the person's mobile phone is in the particular part of the world we would expect this person to be.

This is interesting because – and this is what we found with our paper on digital identification – with all this digital information, you can be much more accurate than in the analogue world.

You previously mentioned the rise of crypto – or virtual – assets. Do authorities need to take more action in this regard?
Marcus Pleyer: Crypto assets are very attractive to individuals and businesses because of their speed and global reach but, at the same time, they are attractive to criminals and terrorists. In the past decade we have seen extensive use of crypto assets for a range of crimes.

Just before this interview, I looked up numbers that [cryptocurrency research firm] Chainalysis provided. They found that, in 2021, more than $14 billion was connected with illicit crypto addresses. This is a huge increase if you compare it with past years.

The FATF issued new standards on digital assets in 2019; we were the first binding standard-setter in this area. We reviewed progress twice, most recently in 2021, and found less than half of countries worldwide reported they had the necessary legislation in place to implement these standards.

So we are still far away from global, coherent regulation of virtual assets, but this is what we need. It is so clear that a virtual asset is a tool that can be easily used across borders, so the risk of leaving loopholes is high, the risk of regulatory arbitrage is very high. FATF is pushing countries very hard to implement our new standards.

Our strategy is to perform mutual evaluations of countries. We will focus on whether countries have implemented these new standards, and if they have not, we have processes in place to address this.

Marcus Pleyer

How much of a problem is it for authorities to trace crypto assets when they are used in illicit activities?
Marcus Pleyer: It depends on the assets. Bitcoin is something you can very easily follow. But then there are these ‘mixers’ that mix virtual assets, which then make it more difficult to follow the trace. Take a case of a ransomware attack where the ransom was collected in bitcoin and then the bitcoins were exchanged into monero. It is then more challenging for law enforcement to follow that trace.

How important is co-operation between different authorities, both domestically and internationally? Do authorities need to put more effort into improving co-operation?
Marcus Pleyer: Co-operation is absolutely vital between agencies and internationally. It is important for the national AML/CFT co-ordinating agency to have a national AML/CFT information-sharing strategy.

There are so many agencies involved in each jurisdiction, and not only the agencies; it starts with the private sector, which is patrolling the first line of defence. Sometimes we go into a country and hundreds of agencies are involved in AML/CFT. They all need to talk to each other. So co-operation is absolutely vital, and this is why the FATF encourages countries to facilitate interagency and public-to-private information sharing.

We have seen great initiatives, for instance in the UK with the Joint Money Laundering Intelligence Taskforce. I think these kinds of public-private partnership can pave the way for information-sharing at a cross-border level.

You previously noted there can be tension between AML enforcement and privacy laws. Is there a way to resolve – or at least mitigate – that tension?

Marcus Pleyer: I don't see this as tension if we work together. Both issues are important policy objectives and they can be compatible.

On one side, we need to fight money laundering/terrorist financing effectively and, for that, supervisors need more data than is sometimes available to them. Being able to access relevant data held by other parties can help a lot. If banks can get a fuller picture of their clients' activities through collaborative analytics, for example, then they are much more likely to detect suspicious transactions.

On the other side, privacy and data protection comes from human rights, a very important issue – especially for me as a European president [of the FATF]. Both are significant public interests that serve important policy objectives. They are not mutually exclusive. For that reason, I have started a project that looks into ways digital technology can help us reconcile these important issues.

This is about encryption technologies, which can allow the responsible sharing of data while upholding a high level of data protection. There are other technologies we have learned about through this project; for example, travelling algorithms – you don't pool the data but the algorithm goes to one bank, looks at the data, then migrates to the next bank. If it finds any strange connections, it raises the alarm.

You mentioned co-operation, which we usually think of as co-operation between AML agencies. But we also need co-operation between the different 'bubbles': the bubble of AML people, the bubble of technology developers and the bubble of data protection people. These people need to work together on solutions.

Has there been much progress in that regard?

Marcus Pleyer: We started this project a year ago when we brought these people together. They are now sitting in one room and working on a solution. But it is complicated. We are a global organisation trying to find best practices that are valuable for all our jurisdictions with their very different cultural and legal backgrounds.

The technology is developing. At the beginning of the project, we heard people say they had the idea but it still needed development. Now it is emerging. In German we say "it's still in children's shoes".

Are there particular things central banks should be doing to improve their AML/CFT oversight?

Marcus Pleyer: As supervisors, central banks monitor financial institutions' activities, risk exposure and the implementation of AML/CFT regulation, at least in some parts of the world. The data gathered during supervisory activity is crucial to the identification, assessment and understanding of AML/CFT risks at a national level.

Even in cases where a supervisor is only supervising prudentially, it is very important they co-operate with the AML supervisor. AML supervision does not work in an independent room – it needs to be connected with information from the banks.

Data must be gathered, assessed and analysed effectively. It must be done in a way that improves money laundering/terrorist financing risk understanding. I think there are some things that central banks could do – one thing I mentioned earlier is that supervisors need to understand the technology that banks use to mitigate money laundering/terrorist financing risk. More and more technology people are needed, not only classical supervisors who can read balance sheets, but also people who understand how AI works.

Central bank digital currency (CBDC) must have financial integrity by design. Some say virtual assets are digital cash, but that is not true. Digital money will always leave a trace and, for that reason, if a central bank issues CBDC, they must ensure this money cannot be misused for money laundering or terrorist financing.

Might the issuance of CBDC assist with AML efforts, if it brings transactions from the crypto industry into the central bank's own systems?

Marcus Pleyer: Yes, of course. If I as a consumer can choose between virtual assets issued by some private company or a virtual asset issued by the central bank, my confidence is much more with the central bank. Money is all about trust. The trust will be much higher with central bank-issued digital money, I think.

You mentioned a need for CBDC not to be exactly cash-equivalent. I think many central banks are now moving in that direction, towards some sort of trade-off between pure anonymity and the need to tackle AML/CFT risks. Is there an upside to the declining use of cash from an AML standpoint?

Marcus Pleyer: There are different cultures in different countries. Some stick very much to cash, and cash is an expression of freedom in many countries, so that is something we have to respect. On the other side, we know that cash can be misused, and we see from Europol and other surveys that cash is still king.

For that reason, the FATF is not pushing countries to abolish cash, but just to address the risks that are involved with using cash. That can be addressed by reporting above a certain threshold, and so on. If people move more into the digital area, it's easier to detect money laundering/terrorist financing. But we have to respect jurisdictions that still want to use cash as they have always done.

You previously mentioned the proliferation of AML/CFT challenges. Are you optimistic the situation will improve in the coming years?

Marcus Pleyer: I would not be in this position if I were not an optimist, but of course it is a never-ending battle. As long as there is money there will be money laundering.

What I can say is our members, in the past 30 years, have improved their AML/CFT systems incredibly, especially when it comes to what we call 'technical compliance'. They have implemented our standards to a great extent into law.

Where we still see a lot of room for improvement is in applying these rules on the ground, what we call 'effectiveness'. That is something we are concentrating on in our new round of mutual evaluations. We are currently in our fourth round, which will come to an end in the next one to two years, depending on the pandemic. Then we will start a fifth round, evaluating all 200 jurisdictions. We will have increased focus on measuring the effectiveness of their systems.

Money laundering fuels serious crimes and, for that reason, it is important that all jurisdictions effectively implement our standards. ❑