BIZWEEK

Economy | Business | Finance

bizweek.mu | ISSUE 606 | SUNDAY 06 SEPTEMBER 2026

SPECIAL ISSUE

8th Annual Mauritian Financial Crime Conference, hosted by Academy of International Finance in partnership with Comsure Compliance Ltd

Nataraj Muneesamy,
Assistant Director of Public Prosecutions

"Public & private sectors must collaborate against financial crimes"

Shammeem Abdoolakhan,
Director of Talent & Technical Development – Axis Eruditio Ltd

"Criminals innovate continuously, and so must Mauritius"

Andy Jarvis,
Co-Founder and Chief Digital Officer of Elevated eXperience

"Legacy systems are leaving the door open to financial crimes"

Shawn Robert Duthie,
Director at Control Risks - South Africa

"Mauritius is not a place where you can hide illicit funds"

Communiqué

Beware of fraudulent content impersonating IBL and its Group CEO, Mr. Arnaud Lagesse

IBL has noticed several fraudulent images and videos circulating on social media that misuse IBL's name and logo and feature AI-generated representations of its Group CEO, Mr. Arnaud Lagesse, to promote fake investment schemes.

IBL hereby draws the attention of the public that these images and videos are fake. Neither IBL nor its Group CEO has any connection with, or has endorsed, the schemes being promoted.

Neither IBL nor its Group CEO requests investments, payments, personal information or banking details through unsolicited social media videos, direct messages or unofficial online platforms.

Members of the public are strongly advised not to click on links, transfer money or share personal or banking information. Report any suspicious content directly through the relevant social media platform. Any investment-related communication claiming to come from IBL should be verified through our official website and social media channels.

Anyone who may have transferred money or disclosed sensitive information should report the matter immediately to the Police and contact their bank or financial institution.

IBL has reported the identified content to the relevant authorities and social media platforms. Members of the public are advised to exercise caution when relying on such posts.

2 September 2026

IBL TOGETHER

iblgroup.com

Making financial integrity an everyday practice

The credibility of an international financial centre is earned through the decisions its institutions make each day. It depends on whether a suspicious transaction is questioned, whether those behind a corporate structure are properly identified, and whether concerns lead to action. For Mauritius, these are matters of economic confidence as much as regulatory compliance.

This was the central challenge examined at the 8th Annual Mauritian Financial Crime Conference, held on 2 and 3 September 2026 at Hilton Mauritius Resort and Spa. Organised by the Academy of International Finance in partnership with Comsure Compliance Ltd, with Bizweek as media partner, the conference focused on "Financial Crime Prevention and Detection in the Digital Age". The articles and interviews in this special issue consider what that ambition requires in practice.

Mauritius has devoted considerable effort to strengthening its framework for combating financial crime. The task now is to ensure that these safeguards work effectively across the system. Risk assessments must shape decisions. Suspicious transaction reports must produce useful intelligence. Information gathered through supervision and investigations must help institutions identify weaknesses and improve their response. Preparation for international scrutiny should be the result of sustained work, not a periodic exercise.

The contributions gathered here show how easily gaps can persist between formal procedures and everyday conduct. An employee may recognise a concern without knowing how quickly, or through which channel, to escalate it. A professional involved in a property transaction may assume that another intermediary has verified the source of funds. A board may receive reassuring statistics without asking whether staff feel able to challenge a profitable client. These are weaknesses that leaders must be prepared to examine honestly.

Technology makes that examination more urgent. Artificial intelligence offers considerable potential to detect unusual patterns and support investigations. It also provides criminals with new ways to deceive, impersonate and operate at scale. Institutions investing in digital tools must therefore pay equal attention to data quality, connected processes and human judgement. Automation is useful only when organisations understand what it detects, what it misses and who is responsible for acting on its findings.

The same discipline must extend across sectors and borders. Banking, fiduciary services, real estate and waqf governance present different risks and require informed, proportionate responses. Mauritius's international connections make cooperation especially important. Public authorities and businesses need practical channels through which to exchange information and expertise, while investigative bodies must have the resources and capabilities to use them effectively.

One priority emerges clearly from these discussions: financial integrity must become a responsibility exercised throughout organisations and sustained between them. Protecting legitimate investment requires institutions that understand risk, exercise sound judgement and act with confidence.

The conference provided an opportunity to question established practices. What matters now is whether those questions lead to better decisions, stronger cooperation and demonstrable results.

BIZWEEK

Economy | Business | Finance

Founder and Editor-in-Chief : Rama Krishna (Rudy) Veeramundar
Editorial Team : Herrsha Bhoyroo, Shareenah Kalla, Jameer Yeadally and Klyven T. Veeramundar
Contact us: Newsroom: bizweekmu@gmail.com
Address: 5th Floor. ICONEBENE -Zendõ, Rue de L'institut, Ebène 72201, Mauritius
Mobile / WhatsApp: 52 53 45 75

bizweek.mu

SHAMMEEM ABDOOLAKHAN, Director of Talent & Technical Development – Axis Eruditio Ltd

"Criminals innovate continuously, and so must Mauritius"

As financial crime evolves at unprecedented speed, Mauritius faces a new challenge: turning a stronger AML/CFT framework into demonstrable effectiveness. Speaking to us at the 8th Financial Crime Conference at Hilton Resort & Spa on September 2 and 3, Shammeem Abdoolakhan stresses that the focus must now shift beyond policies and regulatory compliance towards risk ownership, better-quality information, smarter technology and stronger governance. With AI, digital assets, complex structures and sophisticated fraud reshaping the threat landscape, he argues that Mauritius must ensure its defences evolve as quickly as the criminals seeking to exploit them.

Financial crime is becoming more sophisticated. From your perspective, what are the biggest emerging threats that financial institutions and fiduciary businesses in Mauritius need to prepare for today?

The biggest threat today is not simply the sophistication of criminals—it is the speed at which criminal methodologies evolve. We are seeing greater use of technology, artificial intelligence, digital assets, increasingly complex corporate structures, trade-based money laundering and sophisticated fraud schemes.

For fiduciary businesses in particular, the risk is that legitimate structures and professional services can be misused to obscure ownership, move illicit funds or create an appearance of legitimacy.

We therefore need to move beyond asking, "Are we compliant?" and ask, "Do we genuinely understand the risks to which our business, our clients and our structures are exposed?"

Mauritius has invested heavily in strengthening its AML/CFT framework. How confident are you that the country has moved from regulatory compliance to a genuine risk-based culture within businesses?

Mauritius has made significant progress in strengthening its legislative and regulatory framework earlier this year. But legislation is only one part of the equation.

The real test is whether AML/CFT has become embedded in the decision-making culture of businesses—from the boardroom to the front line.

A genuine risk-based culture means that businesses are prepared to say no to a client or transaction when the risk cannot be adequately managed, even where that decision may have a commercial cost.

I would say Mauritius has moved considerably in that direction, but the journey is not complete. The next stage is about demonstrating effectiveness, consistency and ownership of financial crime risk—not simply producing policies and procedures.

Technology and AI are transforming financial crime. Are Mauritian institutions sufficiently equipped to detect increasingly sophisticated fraud, money laundering and other forms of financial crime, or are criminals still one step ahead?

Technology is both an opportunity and a threat. AI can significantly improve transaction monitoring, customer-risk assessment, anomaly detection and investigative capabilities. But criminals have access to the same technology.

We are already seeing how technology can make fraud more convincing, identities easier to manipulate and financial crime networks more

Cont'd on page 5

difficult to detect.

The answer is therefore not simply to buy more technology. Institutions need quality data, appropriately trained people and intelligent use of technology.

Ultimately, technology should augment human judgement, not replace it. The institutions that will be most effective are those that combine technology with experienced compliance professionals who understand the underlying risks.

The quality of beneficial ownership information remains critical to financial crime prevention. What are the main challenges fiduciary companies face in establishing the true beneficial owner behind complex corporate structures?

Beneficial ownership remains one of the most difficult areas because the legal owner is not necessarily the person who ultimately controls or benefits from a structure. The challenge becomes greater when we have multiple jurisdictions, layers of companies, trusts or other legal arrangements.

The key is to avoid treating beneficial ownership as a box-ticking exercise. A fiduciary should be able to explain, in practical terms: Who ultimately owns this structure? Who controls it? Who benefits from it? And does the explanation make commercial and economic sense?

The law in Mauritius has been amended so that a register of beneficial owners is maintained (not a public register) but based on a strict definition of BO/UBO, we may be the real person/individual behind the structure.

The cost of compliance continues to rise. How can fiduciary and corporate service providers strike the right balance between robust AML/CFT controls and maintaining Mauritius' competitiveness as an international financial centre?

Compliance is undoubtedly expensive, but the cost of inadequate compliance is potentially much greater—not only in terms of regulatory sanctions, but also in terms of reputational damage and loss of confidence in the jurisdiction.

The answer is not to reduce standards in order to remain competitive. Mauritius should compete on quality, integrity, transparency and professionalism.

At the same time, regulation must remain proportionate and genuinely risk-based. We should not create unnecessary compliance burdens where they do not address a meaningful risk.

The objective should be smarter compliance, not simply more effective compliance.

International scrutiny of Mauritius remains intense, particularly ahead of future AML/CFT assessments. What are the areas where you believe Mauritius still needs to demonstrate tangible progress?

I think the emphasis now has to be on demonstrating effectiveness rather than simply demonstrating that legislation exists.
We need to demonstrate that suspicious activity is being identified and acted upon, that beneficial ownership information is reliable, that enforcement is effective and proportionate, and that sanctions and other measures have a genuine deterrent effect.

We also need continued consistency across the different sectors of the financial services industry. International assessors will ultimately

be interested not only in what our laws say, but in what happens in practice.

There should be synergy between the various regulatory authorities to ensure we are not leaving any room for any aspect of supervision to fall through the cracks.

The message should therefore be: Mauritius has built a stronger framework; now we must demonstrate that the framework works.

What should be the priority for the financial services industry over the next three years? Should the focus be on stronger regulation, better technology, greater enforcement—or fundamentally changing the culture around financial crime risk?

I would not choose between regulation, technology, enforcement and culture. We need all four—but culture should sit at the centre.

Regulation establishes the standards. Technology gives us better tools. Enforcement provides deterrence. But culture determines how seriously financial crime risk is actually treated.

Over the next three years, I would prioritise three things: better quality information, smarter use of technology and stronger ownership of financial crime risk at board and senior-management level (i.e good and strong governance in relation to AML/CFT/CPF).

Ultimately, our objective should be to reach a point where AML/CFT is not viewed as a compliance function sitting alongside the business, but as an integral part of how a responsible financial services business operates.

The question for Mauritius is no longer whether we have the laws, regulations and frameworks. The real question is whether we are using them effectively to identify, prevent and disrupt financial crime. In the digital age, compliance cannot stand still. Criminals innovate continuously, and so must we.

NATARAJ MUNEESAMY, Assistant Director of Public Prosecutions

“Public & private sectors must collaborate against financial crimes”

- **“The private sector encounters risks and operational realities that prosecutors or investigators may not necessarily see from their own perspective. That exchange of information is therefore essential.”**

Technology is fundamentally changing the nature and scale of financial crime. Criminals who once had to focus on individual victims can now use automation, scripts, bots and artificial intelligence to target hundreds or even thousands of people simultaneously. Identity theft, electronic-signature fraud and increasingly sophisticated deepfakes are further complicating the task of financial institutions, investigators and prosecutors. For Nataraj Muneesamy, Assistant Director of Public Prosecutions, this constitutes a “silent epidemic” that transcends national borders. His assessment is also clear on Mauritius: the country does not necessarily need more legislation, but it must ensure that its law-enforcement agencies have adequate staffing, expertise, technology, software and training. Speaking to Bizweek during the 8th Annual Mauritian Financial Crime Conference, he also makes the case for more candid and practical cooperation between the public and private sectors.

Why do you describe digital financial crime as a “silent epidemic”?

When we talk about criminality, people subconsciously tend to categorise different forms of crime and assign them different degrees of priority or seriousness. Take murder, for example. In people’s minds, that belongs to one category. Theft or financial loss may be perceived differently, while having an account hacked might be placed in yet another category. What we do not always realise, however, is that these categories are increasingly merging.

Someone could, for example, be murdered because criminals wanted to steal that person’s money or gain access to his bank accounts. What I am saying is that these different forms of criminality are becoming interconnected. Financial crime can be a predominant element even where other forms of criminality are involved. Why do I call it a “silent epidemic”? Because technology is now everywhere. We are having this conversation using a highly sophisticated piece of technology that, not so long ago, could have featured in Star Trek. Yet today, it is simply part of everyday life.

What we tend to overlook is not only how omnipresent technology has become, but also how accessible it is to everyone, including criminals.

Criminals are essentially doing what everyone else does: they use the tools that are readily available to them. The difference, of course, is that they use those tools to commit crimes. We all use artificial intelligence nowadays. ChatGPT is one example. You buy an iPhone and AI is already embedded in it. Google has AI. It is everywhere, and we increasingly take it for granted.

But criminals have access to exactly the same technologies. If you look at criminal activity today, particularly offences involving financial gain, what we broadly describe as financial crime, you will increasingly see technology being used. Artificial intelligence is one example, and a relatively recent one, but this phenomenon is certainly not confined to AI.

How has technology changed the scale at which these crimes can be committed?

Take hacking. Increasingly, hacking involves automation. Criminals use scripts and bots capable of repeatedly carrying out a series of tasks without requiring someone to perform each operation manually.

Cont’d on page 7

Traditionally, a criminal would have had to concentrate his attention on a particular victim. If I wanted to steal money from you, for example, I would have had to focus my efforts specifically on you. Automation has completely changed that equation. A criminal operation can now target ten, a hundred or a thousand people simultaneously.

That is happening in Mauritius, and it is happening around the world. There is another important consequence of technology's global reach. The criminals targeting us are not necessarily Mauritian, nor do they necessarily operate from Mauritius.

They can be located abroad, and once they obtain the money, it does not necessarily remain in Mauritius. It can be siphoned out to other jurisdictions through various sophisticated structures.

The phenomenon is becoming increasingly prevalent, and its scale continues to grow.

How sophisticated and organised have these criminal operations become?

To understand the scale involved, we can look at developments elsewhere in the world.

The United Nations Office on Drugs and Crime reported in September 2025 on trends in criminality linked to digital technology and technological innovation in Southeast Asia.

In that region, you have what are commonly described as scam farms. These operations can involve a hundred or more people working systematically to scam victims, hack into their accounts, obtain their passwords and circumvent the security measures designed to protect them.

And this is not unique to Southeast Asia. Similar activities can be found in Eastern Europe and elsewhere. I am using one region as an example, but the phenomenon exists around the world. That is precisely why I describe it as an epidemic: it is spreading.

Yet, we do not necessarily talk about it in those terms. We talk about epidemics such as Ebola, for example, and focus on the number of victims they have claimed. But we do not necessarily talk in the same way about the victims of financial crime, whose numbers could run into the hundreds of thousands, if not more.

Technology is facilitating this expansion to a considerable degree, and the growth could potentially become exponential. These criminal operations are not simply about one person sitting behind a hundred computers.

You can have a thousand mobile phones and a thousand SIM cards. You can have scripts and bots carrying out repetitive tasks automatically, without someone having to sit behind a screen and perform every operation individually. And now artificial intelligence is also being used to power scams and other criminal activities.

The consequence is that criminals' access to potential victims has increased dramatically. The internet and online services are used by people all over the world. Criminals can therefore exploit that same global connectivity to reach potential victims virtually anywhere. That is why I chose the expression "silent epidemic". We are not necessarily recognising it as an epidemic. I think we should.

What forms of digitally enabled financial crime are prosecutors increasingly encountering?

We are increasingly seeing identity theft. Someone can assume the identity of the legitimate owner of a bank account and then issue instructions, for instance, to a management company or another third party to transfer $100,000 to a particular account.

> **It is not enough to decide at one point that an institution has sufficient people, technology or expertise.**

Essentially, that person has stolen someone else's identity in order to authorise a fraudulent transaction. When I started, someone attempting that type of fraud would have had to forge a physical document, perhaps by reproducing another person's handwriting or signature.

Today, the situation is very different. We use electronic signatures, and those signatures can potentially be forged. Companies and financial institutions have therefore developed additional verification mechanisms. They may conduct a callback and say: "We want to make sure that it was really you who signed this document."

They may telephone the client or arrange a video call to verify that the instruction genuinely came from that person. But the use of artificial intelligence and deepfake technology is creating another level of difficulty. We are seeing trends around the world, not necessarily in Mauritius at present, involving the use of deepfakes to emulate someone's voice.

Deepfake technology can also emulate a person's appearance. There is no reason to believe that Mauritius will necessarily remain unaffected by these developments.

This creates significant difficulties for legitimate companies and financial institutions that are trying to establish the true identity of their clients before authorising a transaction. Technology is making that verification process increasingly challenging.

How should prosecutors and law-enforcement agencies respond to this technological evolution?

At the moment, I think we are still coming to terms with what is happening. We are increasingly becoming aware of these developments, and they raise questions that I ask myself as a prosecutor. They are also precisely the sort of issues we need to discuss at conferences such as this one. But I believe solutions exist.

A good example is the EncroChat case in Europe three or four years ago. EncroChat involved specially equipped mobile phones that criminals could purchase. When switched on, the device could appear to be an ordinary mobile phone. But through a particular code or interface, users could access an encrypted communication platform. Through that network, criminals could communicate securely with one another. They could use it, for example, in connection with drug trafficking, arranging purchases, pickups, drop-offs and other aspects of their criminal activities. It was, in a sense, comparable to the dark web in that criminals could find one another and communicate through what they believed was a secure network without anyone being able to decrypt their conversations. The investigation, as I recall, involved the Dutch police and subsequently cooperation with other European law-enforcement agencies. They managed to infiltrate the EncroChat network, identify users and proceed with arrests. It was estimated that EncroChat had around 60,000 users.

The important point is that this was an example of criminals using technology to their advantage. But it was also an example of law enforcement finding a way to penetrate and dismantle a technology-enabled criminal network. So I believe solutions exist.

In the same way that criminals are using artificial intelligence and other technologies to facilitate the commission of offences, law-enforcement agencies will have to invest in technology, including AI, to improve their ability to detect those crimes. We need to be proactive, perhaps even more proactive than the criminals themselves. Otherwise, it will become increasingly difficult to stop them.

You also mentioned the importance of public-private partnerships. Why is that necessary?

This is something we talk about a great deal, both in Mauritius and abroad, but I do not think we always see enough practical action. Law-enforcement agencies and regulators need to engage with the private sector and work towards common solutions.

Financial institutions, management companies and legitimate businesses do not want to participate in criminal activity, nor do they want their organisations or systems to become the means through which someone is able to commit or facilitate a crime.

By talking to these organisations, law enforcement can better understand the problems they encounter and identify pragmatic and constructive solutions to the growing threat posed by financial crime involving digital devices and technological innovation.

The private sector encounters risks and operational realities that prosecutors or investigators may not necessarily see from their own perspective. That exchange of information is therefore essential.

How useful are conferences such as this one in facilitating those exchanges?

They are very important. I think a prosecutor needs to leave his office every now and then because we need to remain in touch with reality and understand what is happening on the ground.

In my field, "on the ground" means understanding what management companies and people working in the financial sector are thinking and experiencing. These conferences enable us to do exactly that.

You hear about issues that you might not otherwise have considered. For example, during the conference we heard people discussing the difficulties they face in determining whether they should file a suspicious transaction report.

They also have to decide how quickly such a report should be filed. These are very practical problems for the people dealing with them on a daily basis. They are not necessarily issues that prosecutors think about from the same perspective.

It is therefore useful to understand the difficulties faced by the industry, to hear its perspective and to listen to the suggestions it may have. There is always something valuable to emerge from these exchanges.

From a legislative perspective, is Mauritius keeping pace with technological developments?

My personal view is that Mauritian legislation is up to date. We have discussed this before. You can spend all the time in the world legislating and legislating, but ultimately what you need is a sound body of legislation that enables law-enforcement agencies to take action.

The legal framework must allow crimes to be detected, promote their prevention and enable victims to obtain justice. In Mauritius, I think we

Cont'd on page 8

have the necessary laws.

The question, therefore, is not really whether we should legislate more. The more important question is whether we have the resources required to address the threat effectively.

When you talk about resources, are you referring to human resources?

Human resources are certainly a major part of it. From the perspective of government and law enforcement, you need an adequate number of staff. But it is not simply a question of numbers. The quality of those human resources is equally important and there is another aspect that matters greatly: retention. You have to be able to retain your staff. We also need to think about their welfare. I often cite Singapore as an example. Our Singaporean colleagues are very well paid, and their well-being is a matter of concern both to their hierarchy and to the government.

These are considerations we need to take into account. You need to create an environment that enables people to work effectively, but also one in which they actually want to remain. This is a very stressful job. If you invest in people's skills and expertise but cannot retain them, you ultimately weaken the institution's capacity.

Does the question of resources extend beyond staffing?

Absolutely. Resources also mean technology. We need the technology. We need the appropriate software. And we need the training that comes with it. These elements cannot be considered separately. There is little point in acquiring sophisticated technological tools if the people who need to use them have not received the necessary training. As criminals' technological capabilities evolve, those available to law enforcement must evolve as well.

Could public-private cooperation help compensate for some of the expertise or resource constraints within the public sector?

One of the most important benefits of a public-private approach is that it helps you understand what you actually need. There are things we know, and there are gaps in our knowledge that we are aware of. But, there are also things we do not even realise we do not know. That is an important distinction.

The only way to identify some of those blind spots is by talking to colleagues in the private sector. Once that dialogue takes place, you are in a better position to identify a specific set of needs. You can then ask the relevant questions: Do I need to train my colleagues, or myself, in a particular area? Do we need new software? Are there new tools or different ways of working that could improve what we do? The first step is understanding where the gaps actually are.

Could AI itself become one of the tools used by prosecutors?

Yes. There are already tools available that could make our work easier and more efficient. There is a company in the United States, for example, that is developing artificial intelligence specifically for lawyers, including prosecutors. I have friends working abroad, including in Amsterdam, who use this type of technology. They tell me that it is genuinely helping them in the work they do.

Of course, human intervention remains essential. You still need a person to review and double-check everything. AI does not remove that responsibility. But, it can facilitate the work and take care of a significant portion of the workload that lawyers otherwise have to deal with.

The tools are out there. We need to identify those that can help us, determine how they can be integrated appropriately and use them to perform our work more efficiently.

By the time this interview is published, the conference will be over. What would be your main message following these two days of discussions?

I would highlight three things. First, we need to be aware of the crimes that are happening today and understand how those crimes are being committed, and when I say that, I do not mean only criminal activity taking place in Mauritius.The reality today is that we can be affected by all types of criminality, even when the activity originates elsewhere in the world.

Mauritius is an important international financial centre. We are connected to the world, and there is no doubt about that. That means developments and criminal activities elsewhere can have consequences for us.

Second, I think we need to talk more honestly to each other, particularly between the public and private sectors.

We need candid dialogue about what each side is experiencing, the threats we face and the practical solutions that can be developed together. Third, we must not overlook the importance of adequate staffing and resources.

These requirements also need to be reviewed constantly. It is not enough to decide at one point that an institution has sufficient people, technology or expertise. We need to keep reassessing those capabilities to ensure that we are where we want to be and that our law-enforcement agencies can operate efficiently.

Those would be my three principal takeaways.

> **We need to keep reassessing capabilities of our ressource to ensure that we are where we want to be and that our law-enforcement agencies can operate efficiently.**

SELECT

Home Loan

Own your style.

Tailored rates just for you.

From 5.24% p.a.*

*Interest rates vary based on loan amount.
APR as from 5.34%.

MCB is authorised and regulated by the Bank of Mauritius. Terms and conditions apply.

select.mcb.mu

MCB

SHAWN ROBERT DUTHIE, Director at Control Risks - South Africa

"Mauritius is not a place where you can hide illicit funds"

Financial crime does not disappear under stronger regulation - it evolves. For Shawn Robert Duthie, Director at Control Risks in South Africa, financial crime is a moving target and the real test for Mauritius is whether criminals believe they can still exploit its financial system without consequences. Having emerged from the FATF grey list, Mauritius has strengthened its AML/CFT framework, but the next challenge is effectiveness, according to Shawn Duthie. From illicit cross-border flows and prediction markets to AI-driven crime and opaque ownership structures, Shawn Duthie warns that "staying ahead requires constant adaptation, intelligence and enforcement."

You argued that stronger regulation does not automatically reduce financial crime risk, but often changes how it manifests. How should financial institutions adapt when criminals continually shift towards the path of least resistance?

I think financial institutions have to do the same thing, that is, to adapt as well.

Like I said, there is never a point where you can say, *"we have our controls in place, we're done and we can move on to something else."* Compliance departments have to constantly adapt and be prepared for what comes next.

If your compliance department is not on top of developments in AI, finance, crypto, blockchain and everything else that is emerging — and is not trying to stay two years ahead — that is where the stumbling block lies.

Criminals and people involved in illicit activities are ahead of the game. Financial institutions therefore have to do the same.

FATF assessments are increasingly focused on effectiveness rather than formal compliance. So what concrete outcomes should Mauritius demonstrate to prove that its AML/CFT framework is delivering results?

I think Mauritius is actually in a better position than South Africa, for example, and even Namibia, because it really took the grey-listing experience to heart and made a lot of changes.

Mauritius was, I believe, one of the fastest jurisdictions to come off the grey list — in about a year and a half. South Africa was on it for around three years. So, obviously, the controls are in place and things are working.

What they will want to see is whether behaviour has changed. They want to see that people no longer look at Mauritius and think, *"We could go there and perhaps do something."*

Instead, they need to know: *"Mauritius is not a place where we can do this because, if you do, you will be caught, charged and punished."*

As long as Mauritius continues on the same path, I think that, even with the peer review in early 2027, it will probably be fine.

You warned that Mauritius' role as a financial bridge between Africa and Asia is both an advantage and a vulnerability. Which cross-border financial crime risk should the country be watching more closely?

I mean, it is obviously hard to kind of pinpoint just one. I think where the issue is going to be is the wider aspect of financial crime. So there are obviously, I think, probably quite a few transactions between Dubai and Mauritius, for example, and probably the vast majority of these are completely legal.

But what you want to then look at is what is the wider story behind those transactions. I mean, I use the example of Zimbabwean gold smuggling, but I'm sure if you looked at diamond smuggling or copper smuggling or cobalt smuggling from Congo or Zambia, through Rwanda into Dubai, back to Mauritius and then back into the continent, I mean, there are all these tiny areas that compliance officials are going to have to look into.

It is not just going to be what we have to monitor Dubai, they monitor us, that's it. You have to look at the wider scheme of what's happening in the broader ecosystem of the financial transaction.

Banks have traditionally been at the centre of financial crime controls, but attention is shifting towards lawyers, accountants, real estate professionals, corporate service providers, and virtual asset businesses. Where do you currently see the most significant regulatory gaps?

I think the biggest regulatory gaps are going to be in those areas.

People do not always recognise that lawyers and attorneys can be important cogs in financial crime. They can obviously become involved in these activities.

Real estate has also long been recognised as an easy way to hide and layer funds, although that is becoming more difficult.

I think the bigger issue now is new technology — digital money transfers, cryptocurrency, online gambling and prediction markets such as Polymarket.

Some prediction markets argue that they are not really betting and therefore should not be regulated in the same way. But the mechanism is similar: you can put money in, including crypto, win, and then take money out.

That creates another avenue for people to layer or use illicit funds and hide them from regulators and banks.

And, as I said, this is never going to end. Criminals are always going to find a different way to do this. At the moment, these are the areas that need greater regulatory attention.

You identified unregulated prediction platforms as a potential means of layering and concealing illicit funds. How serious is this emerging risk? Should such platforms be regulated in the same way as gambling or virtual asset services?

I think so, yes. I mean, I think at the moment it might be that it is not as big a platform as online gambling, for example. I mean, particularly on the continent.

At the moment, prediction markets may not be as significant as online gambling, particularly in

Cont'd on page 11

Africa. They are still relatively limited here. In the United States, they are very big, and they are also significant in Latin America. In Europe, they are growing.

But people will realise the amount of money that can be made from them and the different ways in which they can be used. It is only a matter of time before that becomes more significant.

Yes, absolutely, they should be treated in the same way we look at online gambling or crypto.

That does not mean we have to stop these activities. We simply have to regulate them.

Beneficial ownership registers have improved transparency, yet criminals can still conceal who actually controls a company. What investigative techniques are most effective in uncovering the individuals operating behind nominees and complex corporate structures?

It is difficult, because unless someone is sloppy, if they do not put their name down, there may not be a paper trail.

If you have a politically exposed person or someone involved in crime, they are not going to say, *"I need that legal shareholder to show that I am the owner."* It is simply not going to happen.

So, when you are looking at a company, you ultimately have to ask: who is really in control? That is something that is never necessarily done on paper. This is where a network of human sources can be extremely important. You can reach out widely, speak to people discreetly and find out what the allegations are.

It is rare that someone will simply say, *"It is this person, and here is all the evidence."* Instead, you get little allegations and small nuggets of information. You may get only a first name or a last name.

Those individual data points can then widen the investigation, leading to more data points and further investigation.

At the end of the process, it is rare to have a smoking gun where you can say, *"Here is the absolute evidence that this person owns that mine."* Often, it is based on probability.

If four or five independent sources are all saying the same thing, the probability of it being true becomes much higher. That is then what we would advise the client.

At Control Risks, we combine open-source intelligence with human intelligence when investigating suspicious individuals and entities.

At what point should an institution move beyond routine database screening and commission enhanced due diligence?

For banks and corporate secretaries, there has to be a risk-based approach. You do not want to spend a huge amount of money conducting extensive due diligence on every single client. But if an issue is identified during onboarding, there has to be a decision: either say no to the client or go deeper into the relationship.

There should also be a link between the level of due diligence performed and any subsequent suspicious activity report or suspicious transaction report.

If you only conducted a basic World-Check screening when onboarding a client and subsequently identify suspicious transactions, you should go back and ask why.

There should be guidelines and controls in place so that when you onboard someone, you have sufficient confidence that they are legitimate.

And if an SAR subsequently emerges, you should reassess the relationship and determine whether further due diligence is required and whether you should continue with that client.

You say that AI has democratised digital crime by giving people with limited technical expertise the ability to create malicious programmes. How should financial institutions rethink their cybersecurity and financial crime controls in response?

As I said before, they have to stay ahead of the game.

One way of doing this is through penetration testing, or what we call a red team — having someone continually try to break into your systems. When they find a way in, you identify the vulnerability and fix it.

Obviously, this is becoming more difficult with AI. We now have systems such as Claude that can be used to break into things very quickly, potentially much faster than a human could.

Ultimately, I think that in the future a human may not be enough to stop it. It could be another AI, specifically programmed and trained to defend against sabotage attacks. That is probably the future we are looking at.

Things are going to move so quickly that you will need something else moving just as quickly to defend against them. The challenge is always going to be: how do you stay ahead of the game?

You concluded that the most serious risks increasingly sit within apparently legitimate activities. So, what warning signs can help businesses distinguish an ordinary commercial transaction from one that forms part of a wider financial crime network?

There are obviously red flags that appear throughout the process. If you are conducting due diligence or a suspicious transaction report emerges, that tells you that something may need to change.

It could be a link to a PEP, a high-risk jurisdiction, or transactions that repeatedly sit just below a reporting threshold. But there is also an element of gut feeling.

If you do this for long enough, you see something come across your desk and think, *"Something is not right here."* We have encountered this during investigations. We have looked at something and said, *"We need to go deeper. Something just doesn't add up."*

That is where I see the advantage of having skilled and experienced investigators, rather than relying solely on AI or people who have only been doing this for a year or two.

There are warning signs you are trained to identify, but ultimately there is also a gut feeling that tells you: we need to go deeper. There is something here that requires further investigation.

Cont'd on page 12

SHAWN ROBERT DUTHIE, Director of Control Risks South Africa

"Better regulation does not automatically mean lower risk"

Shawn Robert Duthie, Director of Control Risks South Africa, warned that organised criminals were exploiting legitimate businesses, non-bank institutions and increasingly connected African payment systems. He said Mauritius's position between Africa and Asia supported investment and trade but also exposed its financial sector to illicit proceeds moving through jurisdictions such as South Africa, Zimbabwe and Dubai. This was day 2 of the 8th Financial Crime Conference at Hilton Mauritius Resort & Spa on September 3.

Mauritius's role as a financial gateway between Africa and Asia places it at growing risk from criminal networks that use legitimate companies, cross-border payment systems and complex ownership structures to conceal illicit funds, according to Shawn Robert Duthie, a director at Control Risks South Africa.

He said stronger regulations had forced criminals to adapt rather than abandon financial systems. As banks and national authorities tightened their controls, illicit activity was moving towards weaker institutions, informal markets and new payment channels.

"Ultimately, criminals will find the path of least resistance," he said. *"As we improve our systems and regulations, they will find other avenues to exploit."*

Duthie, who leads Control Risks' political risk and intelligence work in Southern Africa, was speaking on Day 2 of the 8th Financial Crime Conference at the Hilton Mauritius Resort and Spa. His session examined financial crime trends in Africa and their implications for businesses.

The conference, organised by the Academy of International Finance in partnership with Comsure Compliance, took place on September 2 and 3 under the theme *"Financial Crime Prevention and Detection in the Digital Age"*. It brought together regulators, prosecutors, lawyers and industry specialists to discuss sanctions, banking and real estate risks, asset tracing, artificial intelligence and the effectiveness of anti-money laundering and counter-terrorist financing systems.

REGULATION CHANGES RATHER THAN REMOVES RISK

He identified three principal trends: the transition from rule-based compliance to measurable effectiveness, increased scrutiny of institutions outside the banking sector and the use of regional financial systems to move illicit funds.

> **Increasingly, the most serious risks we find sit within apparently legitimate activity.**

Regulation had improved across Africa, often in response to Financial Action Task Force grey-listing and mutual evaluations. Mauritius strengthened its financial crime framework and secured its removal from the grey list. Namibia was removed in June, while South Africa was confronting the findings of its own review.

But improved regulation did not necessarily make the underlying threat smaller.

"Better regulation has not necessarily reduced risk; it has changed how risk manifests itself," he said. FATF was increasingly likely to assess whether laws and controls produced tangible results, including investigations, prosecutions, asset seizures and changes in behaviour. Simply adopting legislation or demonstrating that institutions followed prescribed procedures would no longer be enough.

In South Africa, Duthie expected attention to turn towards prosecutions arising from the Zondo Commission's investigation into state capture and corruption. *"FATF will ask not merely whether we have followed the rules, but whether there will be prosecutions,"* the director said. *"Will senior leaders against whom there is evidence of financial crime be put in the dock?"*

Financial institutions and companies therefore had to consider whether their systems identified and reduced real risks, rather than measuring success by the number of checks completed.

"One of my principal conclusions is that better regulation does not automatically mean lower risk," Duthie said. "Increasingly, the most serious risks we find sit within apparently legitimate activity."

SMUGGLERS ADAPT TO STRONGER BORDERS

Zimbabwe illustrated how criminal activity could migrate when one route became more difficult. Duthie estimated that about 80 per cent of the country's economy operated informally.

A formal retailer such as Pick n Pay might sell a product at a price expressed in Zimbabwe Gold, or ZiG, that was equivalent to about US$30. Informal roadside shops operating from vans could sell the same product, smuggled from South Africa, for about US$5 plus a margin of 10 or 15 per cent.

Beitbridge had historically been the principal route for moving such goods between South Africa and Zimbabwe. Its operation had improved significantly over the preceding two or three years, making the border crossing faster and more efficient.

That improvement supported legitimate trade but made smuggling through Beitbridge more difficult. Illicit traffic consequently shifted towards other border crossings.

"Criminals will find a way," he said. The pattern demonstrated that closing one vulnerability could displace illegal activity rather than stop it. Risk teams therefore had to monitor how criminal networks responded to infrastructure and regulatory changes.

DRUG OPERATIONS RELOCATE TO AFRICA

Duthie pointed to a similar development in the international narcotics trade. Mexican cartels facing greater difficulty moving drugs into Europe had begun relocating operations to Africa.

Control Risks had identified four or five Mexican-run drug operations in South Africa during the preceding year, he said. Once based there, criminal groups could move narcotics through other African countries and onwards to Europe.

South Africa was attractive partly because of the maturity of its financial system. "I'd say South Africa has probably the most mature financial system in Africa, followed closely by Mauritius," Duthie said. *"That was why South Africa was chosen. It's easier to move money in and out."*

Mauritius faced a related exposure. Proceeds generated in South Africa could move through Mauritius and Dubai before reaching their destination. *"Drug cartels can move proceeds from South Africa through Mauritius and Dubai, using our financial systems to move the money onwards,"* he said.

CRIMINAL ATTENTION EXTENDS BEYOND BANKS

Banks were no longer the sole focus of financial crime regulation or criminal exploitation. Corporate service providers had become increasingly important, while lawyers, accountants and real estate professionals were likely to face greater scrutiny.

Virtual asset service providers were another area of concern. These included cryptocurrency companies, online gambling operators and payment service providers. The director also identified prediction platforms as an emerging vulnerability. Services such as Polymarket allow users to place money on the outcome of future events, ranging from sporting contests to political and military developments.

Users might wager on whether the US would attack Iran or on words used during a political speech. In some jurisdictions, such platforms were not treated as betting services and remained outside conventional gambling regulation.

Criminals could exploit the resulting gap to place funds, layer transactions and make illicit money

Cont'd on page 13

more difficult for banks and regulators to identify.

"As banks strengthen their defences, criminals will find new ways into the system," he said.

AFRICAN PAYMENTS BECOME MORE INTERCONNECTED

The gradual development of the African Continental Free Trade Area and the expanding responsibilities of regional groupings were making finance across the continent more interconnected.

Duthie said much of the progress remained rhetorical, but initiatives such as the Pan-African Payment and Settlement System demonstrated the direction of travel.

PAPSS allows businesses to transact in local currencies. A company sending money or goods between South Africa and Nigeria, for example, does not first have to convert rand into US dollars and then dollars into naira. The transaction can be settled directly in rand and naira.

That is beneficial for trade and cross-border payments. It may, however, also allow transactions to pass through four or five jurisdictions and currencies, layering the transfers and obscuring their origin.

Funds could move from rand into naira, then into kwacha and shillings before reaching their destination. Such a chain would be more difficult to trace than a transfer conducted solely in dollars.

"This is particularly important for Mauritius," Duthie said. "I*t is a financial hub for the continent and, in financial terms, a middleman between Asia and Africa. That is both an advantage and a risk."*

ZIMBABWEAN STRUCTURES INVOLVE MAURITIUS AND DUBAI

Businesses seeking to move money out of restrictive economies were already using cross-border structures. He recalled asking contacts in Zimbabwe how easy it was to conduct business and transfer money abroad. They initially said it was very easy. Their answer changed when he asked how easy it was to move the money legally.

Many Zimbabwean companies were structured through Dubai and Mauritius, allowing them to bypass Zimbabwe, he said. Duthie referred to Al Jazeera's Gold Mafia documentary, in which individuals were filmed discussing how Zimbabwean controls and sanctions could be circumvented through Dubai and Mauritius.

Where a gold company moved money between the two jurisdictions, a financial institution had to consider whether the funds derived from gold smuggled out of Zimbabwe or from another illicit activity.

"We can no longer assess risk through a single-country lens. We must build as complete a picture as possible," Duthie said.

TRADE CAN CONCEAL THE MOVEMENT OF MONEY

Trade-based money laundering was one of the principal typologies encountered by Control Risks. It could involve underinvoicing or overinvoicing goods and using false documentation to hide or misappropriate funds.

Such conduct could threaten not only the integrity of a transaction but also the viability of the company concerned.

Duthie cited Eskom, South Africa's state-owned electricity company, as an example. Sabotage and illicit activity in procurement and other parts of its operations were tolerated until the organisation could no longer function properly.

South African Police Service units were subsequently deployed permanently at Eskom sites around the country. They operated continuously and examined activities rather than limiting their presence to occasional visits.

The intervention had helped the organisation recover, Duthie said. By that stage, corruption, procurement fraud and other forms of theft had inflicted serious damage.

Private companies often approached Control Risks with comparable suspicions. They had not necessarily reported the matter to police but wanted to determine whether misconduct was taking place and how it could be addressed.

Forensic specialists could conduct overt reviews to establish whether prices, volumes and shipping routes made commercial sense. Covert work could then examine relationships between employees in procurement or other sensitive positions and external suppliers.

Investigators asked who owned the suppliers, trucks and warehouses; which other companies the suppliers served; and how their employees and directors were connected.

The critical relationship might sit three layers below the original transaction. A procurement employee could award favourable contracts to a supplier, while the true beneficiary receiving kickbacks was concealed behind several entities.

ONLINE CHECKS CANNOT ALWAYS AUTHENTICATE DOCUMENTS

Document verification presented another challenge. South Africa was relatively advanced in making public information available online. Investigators could, for example, verify an identity number or a marriage electronically.

Equivalent information was not available online in every African jurisdiction, requiring investigators to make in-person inquiries.

Even in South Africa, some documents could not be verified fully through an electronic search. Control Risks conducted due diligence on South African applicants seeking citizenship-by-investment passports from countries such as St Kitts and St Lucia, including checks for concerns they had not disclosed.

Criminal record certificates were among the documents that required additional verification. Artificial intelligence could now help produce a document that looked almost identical to an authentic certificate.

Duthie described a recent case in which he sent

Cont'd on page 14

Better regulation does not automatically mean lower risk.

a junior colleague to Pretoria to present a document for inspection. It was found to be false. The authorities wanted to know where the information had originated and who was involved, although Control Risks could not disclose its source.

"The case shows why you should not simply trust a document viewed online," he said. *"Sometimes you must verify it in person."*

A GENUINE PASSPORT MAY STILL CONCEAL CORRUPTION

The problem extended beyond forged documents. A South African passport or permanent residence document could be genuine and appear correctly in an online government database yet still have been obtained fraudulently.

An individual might have bribed a contact at the Department of Home Affairs 10 or 15 years earlier, paying about US$10,000 to have information entered the system and an official document issued.

The resulting passport or identity document was genuine. Neither visual inspection nor an online check would necessarily reveal the corruption behind it.

Investigators might establish what happened only by asking Home Affairs to retrieve the original paper file from a warehouse and check whether the prescribed process had been followed.

Duthie said Home Affairs had prosecuted employers for hiring people it considered to be in South Africa illegally, even though those employees possessed genuine government documents.

Financial institutions dealing with South African nationals and permanent residents therefore had to consider the integrity of the process through which a document was obtained, rather than relying exclusively on the document and its database entry.

OWNERSHIP REGISTERS CANNOT REVEAL EVERY CONTROLLER

Corporate ownership registers were becoming more transparent in many African jurisdictions. The Director described Mauritius and Botswana as strong examples and said Lesotho might have the most advanced system.

Lesotho's register included shareholders and ultimate beneficial owners and provided high-quality information, he said.

Nevertheless, criminals could still conceal both ownership and, more importantly, control of a company.

Transparency measures improved visibility but did not eliminate the use of nominees, layered entities or informal relationships. This did not mean that governments should abandon beneficial ownership systems, but it demonstrated the limits of relying on registers alone.

"Unfortunately, it is very difficult to prove who actually owns or controls a company," he said. Clients often asked investigators to identify a company's beneficial owners. The connection might be visible when someone had been careless or was only two corporate layers removed. In more sophisticated arrangements, proving ownership or control was considerably harder.

Control Risks used corporate mapping to trace relationships across three or four layers. Where a person served as a director of 20 companies, investigators examined the other directors of those entities, their additional directorships and the people associated with the wider network.

The process could uncover a connection that a direct search had missed.

Lifestyle audits provided further evidence. Investigators assessed whether family members, business partners, nominees and long-standing associates received unexplained benefits or held assets beyond what their known incomes could support.

Human sources could also assist. People close to a family or individuals within an established intelligence network might provide information that increased the likelihood of identifying the person exercising genuine ownership or control.

POLITICAL CONNECTIONS REQUIRE JUDGMENT

Shawn Robert Duthie warned against assuming that if every relative of a politician represented an unacceptable risk. *"A politician's relative is not necessarily a bad person. Relatives still need bank accounts and may need to start businesses,"* Duthie said.

Investigators had to determine whether funds received by a politically connected relative genuinely belonged to that person or were being held or used for an unnamed official.

African clients often faced a higher risk premium. Control Risks worked with US clients that sometimes assumed a subject was corrupt solely because of a relationship with somebody in government.

"You cannot say that everyone involved in African politics is corrupt," Duthie said. He contrasted the scrutiny applied to African political connections with perceptions of wealth accumulation by members of the US Congress. In Africa, even a second cousin of a deputy labour minister might be flagged as a politically exposed person.

The investigator's role was to assess the actual significance of the relationship.

"*A checklist or another government may classify someone as a politically exposed person, but we must decide whether the relationship creates a real risk for the client,"* he said. In some cases, Control Risks found no evidence of a material red flag despite the client's initial concerns. The existence of a political relationship alone was not proof of wrongdoing.

Ultimately, criminals will find the path of least resistance

CASH ECONOMIES COMPLICATE INVESTIGATIONS

Financial conditions differed substantially across Africa. South Africa and Kenya were relatively well banked, while Zimbabwe, Angola and Malawi relied much more heavily on cash.

This reflected limited financial inclusion as well as low public confidence in governments and national currencies.

Criminals could exploit those conditions through mobile-money services, remittances and informal transfer systems. Hawala networks were frequently used to move funds across jurisdictions but could be difficult to identify, prove and investigate.

Conventional screening therefore had to be followed by analysis of what the information meant and whether the proposed business relationship created a material risk.

The source of wealth was often particularly difficult to establish. *"You cannot simply ask Google where a person obtained the money,"* he said. Investigators examined the subject's companies, properties and trusts, together with family and business connections. They constructed a timeline of how the wealth had developed, including when houses and vehicles were acquired and when trusts were established.

The resulting picture allowed them to assess whether the individual's lifestyle was consistent with the declared source and level of wealth.

INTELLIGENCE SUPPORTS RISK DECISIONS

Shawn Robert Duthie said Control Risks combined open-source and human intelligence to give clients strategic insight and support decisions about whether to accept a risk.

A bank or corporate services provider might identify red flags concerning a major prospective client but still want the business. Enhanced due diligence could examine the individual's source of wealth, commercial background, business pathways and wider network.

Human intelligence from Control Risks' contacts could supplement public records where the available documentary information was incomplete. The company also operated VANTAGE, a higher-volume third-party compliance service comparable to screening services such as World-Check and iTrack. The service was partly automated but also drew on analysts and risk assessments across Control Risks' global network of 41 offices.

Duthie distinguished this work from that of a compliance officer. His focus was not on interpreting FATF guidance but on investigating entities and individuals to establish the risks they presented.

The purpose was to provide clients with enough reliable information to decide whether a relationship should proceed and on what terms.

"We have all conducted screening checks," he said. *"The analysis of the data matters most: what is the actual risk if we proceed?"*

The task was not to accumulate the largest possible number of alerts. It was to connect people, companies, transactions and jurisdictions into a coherent picture. *"Financial crime investigations are not about generating the greatest number of alerts or red flags,"* Duthie said. *"They are about connecting people, relationships and businesses so that our clients have the full picture and can make sound decisions."*

NAUSHAAD KHALID MALLECK, Barrister & Chairperson of the Real Estate Agent Authority Board (REAA)

"AML/CFT test will be won in files, not in speeches"

Mauritius is entering a decisive phase in its fight against financial crime, with the forthcoming ESAAMLG evaluation set to test not just the strength of its laws, but their effectiveness in practice. For Naushaad Khalid Malleck, the challenge is clear: results must be demonstrated through evidence, enforcement and changed behaviour. As the real estate sector comes under tighter regulatory scrutiny, he argues that Mauritius must prove its AML/CFT framework works where it matters most, that is, in practice.

You have highlighted how attractive real estate can be to financial criminals. What makes property particularly vulnerable to money laundering?

Property does several jobs for a criminal at once and that is what makes it exceptional. A single transaction absorbs a sum that would take months to move through a bank in structured deposits. The asset does not depreciate, it appreciates, so the exercise pays for itself. It can be lived in, let, or used to run a business. It can be borrowed against, which converts criminal proceeds into a clean bank facility and, over several years, into a documentary history of respectable financing. And another very important thing to understand is that ownership confers standing: a man with an address has a story he can tell.

In our jurisdiction there is a sixth attraction. An acquisition above the prescribed threshold under our property schemes carries a residence permit. That is lawful and deliberate policy and I'm not criticising it, but it means the property here is not only a store of value. It is a gateway to status and to presence.

How significant is that risk in Mauritius today, and where are the main vulnerabilities in our real estate sector?

Our Second National Risk Assessment rates national money laundering risk as Medium-High. It rates the real estate sector Medium-High, with a residual vulnerability assessed as High — and the notaries who sit in the same transaction, Medium-High as well. Those are serious numbers and I would not soften them.

But when one reads the assessment carefully, the diagnosis is a precise one. We have been failing on vulnerability, not on threat. Threat is what the criminal does whereas vulnerability is what we leave open to him. The principal vulnerability of this sector was simply that there was no door at the entrance to it. Anyone could hold himself out as a real estate agent. There was no register, no fit-and-proper test, no bar on a person convicted of a financial crime offence or named on a United Nations sanctions list.

That is a vulnerability we can actually fix, and it is the one the Act has now closed. Not only do we now have a door, but there is a lock.

Property transactions can involve companies, trusts, nominees and several intermediaries. How difficult is it in practice to establish who the ultimate beneficial owner — and the real source of the money — actually is?

The answer is: difficult, and the difficulty is not evenly distributed.

Identifying a beneficial owner on paper is usually achievable. Establishing whether the paper reflects reality is harder and establishing where the wealth came from is harder still.

The distinction that matters is between source of funds and source of wealth. Source of funds is where this money came from for this purchase whereas source of wealth is how the person came to have money at all. A well-advised purchaser can almost always document the first. It is the second where the story tends to break.

Two features make it harder here specifically. The first is the prête-nom (acquisition in the name of a relative, for example) which our own Financial Intelligence Unit identifies as a Mauritian vulnerability and which is culturally so ordinary that it can pass without a second thought. The second is that in a chain of five professionals, each holds one fragment of the picture, and no single one of them holds the two facts that would make the whole thing obvious.

Mauritius has strengthened the licensing and supervision of real estate professionals. What weaknesses is this new framework intended to address, and are there still operators or activities falling outside the regulatory net?

The framework addresses entry, which was the sector's central weakness. Since 1 August 2026, no person may act as a real estate agent unless registered; registration carries a fit-and-proper test and an entry standard; every registered agent must register with the Financial Intelligence Unit; compliance officers and reporting officers are approved by the Authority; a Code of Conduct and Practice has been issued; and failure to report a suspicious transaction is a criminal offence carrying up to one million rupees and five years.

Are there gaps? Yes, and I would rather say so than pretend otherwise. Registration is proceeding in phases: agency work, property development and land promotion first, with rental and the remaining

Cont'd on page 16

activities to follow. And there are operators who have simply never intended to come inside, particularly those advertising on social media, where the barrier to holding yourself out as an agent is a photograph and a telephone number.

That is why the Act has a criminal limb as well as a supervisory one. Unregistered practice is an offence, and an unregistered person cannot sue in any court to recover his fee. We will be pursuing that work with the Financial Crimes Commission. A gate is of no use if walking round it costs nothing!

Real estate involves agents, developers, lawyers, banks and other professionals. When suspicious funds enter a property transaction, where does responsibility lie, and are these professionals sufficiently equipped to identify the red flags?

Responsibility lies with each of them, undivided. It is not shared out and it is not discharged because another regulated professional was also present. Our own Act puts it in these terms for my licensees: the anti-money-laundering obligations are in addition to, and not in derogation from, the Financial Intelligence and Anti-Money Laundering Act.

The practical failure is rarely dishonesty. It is assumption. The agent assumes the notary will verify the source of funds. The notary assumes the bank checked when the account was opened. The bank treats a notarial transaction as lower risk precisely because a notary is involved. The real danger is when everybody has reasonably assumed and nobody has actually looked. The launderer's most reliable ally is not the corrupt professional; those are rare and are eventually caught. It is the honest professional who assumes someone else did the work.

As for how well equipped they are: unevenly. Banks and management companies have mature compliance functions. The agency sector is at the beginning, which is why training and continuing professional development are being built with the Financial Services Institute and the University of Mauritius rather than left to chance.

How do you strike the balance between rigorous AML/CFT controls and keeping Mauritius attractive and business-friendly for legitimate property investment?

I would resist the framing a little, because it treats rigour and attractiveness as opposites. They are not. A market in which prices are distorted by buyers who are not price-sensitive, because they are not really buying, is not an attractive market for anyone trying to trade in it honestly. And the most business-unfriendly thing that can happen to this jurisdiction is a grey listing.

That said, proportionality is real and we take it seriously. Our approach is a blend of regulation and self-regulation. Registration is phased and risk-based. The fee was deliberately set in line with the trade fee licence that preceded it, so that this is a change of regime rather than a new tax. The e-licensing portal was pilot-tested with agents from the sector and their input was taken on board before it went live.

We will not have the optimum mix perfectly balanced from the word go and I do not claim otherwise. But we aim to be business-friendly and we are open to suggestions.

You suggested that if Mauritius were placed on the grey list again, getting off it could take at least two years. Why could the consequences and the process be more difficult this time?

That is not what I said. What I said is that last time it took us two years. This round is about effectiveness

and that will make matters considerably more complicated for any jurisdiction which does not pass and finds itself on the grey list.

The coming ESAAMLG evaluation will not be about the statute book. It will be about effectiveness and effectiveness is demonstrated by evidence accumulated over time: supervision that changed behaviour, reports that produced outcomes, cases that were pursued. You can amend a statute in one sitting. You cannot manufacture years of enforcement evidence.

The consequences would also be less forgiving. A first listing reads, externally, as a jurisdiction still building. A second reads as a relapse, and correspondent banking relationships, once they have narrowed, do not widen again quickly. The friction arrives without announcement and it recedes slowly.

We are now talking much more about "effectiveness". How will the forthcoming assessment differ from the previous one Mauritius underwent? Is having the right laws, regulations and institutions in place no longer sufficient?

Correct. Having the right laws, regulations and institutions is necessary, but not sufficient. The methodology assesses two distinct things. Technical compliance asks whether the legal and institutional framework meets the standard. Effectiveness asks whether the framework produces results and it is measured against a set of Immediate Outcomes rather than against the text of the law.

Technical compliance asks whether the law exists. Effectiveness asks whether anybody has felt it. Practically, that changes what a country must be able to produce. Not an instrument, but evidence and evidence of a kind that cannot be assembled at short notice. It also changes who is examined. Assessors do not evaluate an authority in the abstract. They sit across a table from working supervisors, compliance officers and reporting officers and ask what risks the business faces and what is done about them. The quality of those answers is part of the grade.

Taking all this into account, are you confident that Mauritius can demonstrate that its AML/CFT framework is working effectively in practice and avoid returning to the grey list?

I am confident about the framework. This country has built, in a relatively short period, a legal and institutional architecture that stands comparison with jurisdictions far larger than ours, and the closing of the real estate perimeter this year removed one of the last significant gaps in it.

Confidence about the outcome is a different thing, and it has to be earned between now and 2028. It will be earned in files, not in speeches. Effectiveness is not a quality a jurisdiction announces about itself, it is a finding somebody else makes after examining what we actually did.

What I would say is this: the work required is entirely achievable, it is understood by the institutions that must do it, and none of it depends on anything outside our control.

I would far rather this Authority find its own weaknesses in 2026 than have them found for us in 2028, and if every institution in the chain takes that view, I think we will be in a position to demonstrate what we need to demonstrate.

MATHEW BEALE, Founder and Chief Executive of Comsure Jersey

"Suspicions come from the industry and from its employees"

When an employee notices a suspicious transaction, the next few decisions can determine whether a firm's financial crime controls work in practice. That concern ran through the remarks of Mathew Beale, the founder and chief executive of Comsure Jersey during his opening remarks and presentation at the eighth Financial Crime Conference, held at the Hilton Mauritius Resort and Spa on September 2, 2026. He urged businesses to examine how staff recognise and report concerns, as tighter reporting expectations and the adoption of artificial intelligence put their procedures to the test.

Financial institutions investing in compliance technology face a more basic test: whether an employee who identifies a concern knows how to bring it promptly to the person responsible for assessing it.

That was a central argument of Mathew Beale's contribution to the eighth Financial Crime Conference on September 2 at Hilton Mauritius Resort and Spa. Across his opening remarks and technical presentation, the founder and chief executive of Comsure Jersey examined the distance between having a reporting procedure and knowing that it works.

Organised by the Academy of International Finance in partnership with Comsure Compliance Ltd, the two-day event addressed "Financial Crime Prevention and Detection in the Digital Age". Its programme covered sanctions, banking, property, law enforcement co-operation, governance and the growing role of artificial intelligence.

Mathew Beale, who also served as master of ceremonies, encouraged delegates to participate actively, ask questions and exchange views with speakers and fellow participants. He highlighted the electronic question-submission facility, accessible through a QR code, including the option to raise questions anonymously.

His opening remarks placed the discussions within a transition from paper-based processes to a financial environment increasingly shaped by data. His subsequent presentation brought that transition back to the practical handling of suspicion.

THE UNCERTAINTY BEFORE A REPORT

In his session, *"Suspicion Confirmed: Clock Running: Closing the gaps exposed by FIU"*, Beale welcomed guidance issued by Mauritius's Financial Intelligence Unit. *"I would argue that this kind of guidance is probably one of their better bits of guidance,"* he said.

Clearer guidance, however, also provides more measurable expectations against which a business's performance can be assessed. He questioned whether attention to reporting timetables could leave the behaviour behind those timetables insufficiently examined.

His sharpest concern involved the instruction for employees to report internally *"without delay"*. *"The most dangerous paragraph in this whole handbook is that statement,"* he said.

The difficulty, in his account, is translating urgency into a consistent response across a business. An employee identifying a concern before a weekend, or before attending a two-day conference, may interpret the instruction differently from a regulator examining the sequence of events afterwards.

That leaves firms with an obligation to make their internal expectations intelligible. Detailed deadlines later in the reporting process cannot resolve uncertainty about when an employee should first act.

The Chief Executive emphasised why that initial stage matters: "Suspicions come from the industry, that comes from the employees." The employee's concern and the reporting officer's assessment are distinct parts of the process. Staff must bring forward relevant information; the money laundering reporting officer must analyse it and decide whether an external report to the FIU is warranted.

> **The difficulty, in his account, is translating urgency into a consistent response across a business**

Mathew Beale welcomed the clarification of the timetable's starting point, which he described as the arrival of the internal report with the reporting officer. But the practical consequence is that the preceding handover needs equal attention. The officer cannot assess information that has not arrived.

CAN EMPLOYEES FIND THE FORM?

His examination of reporting controls extended to the everyday organisation of documents. An employee may recognise something unusual but struggle to locate the correct form. Reporting materials can be dispersed across internal systems, leaving staff unsure which document to use. *"Is it version one, version two?"* he asked.

The question is administrative, but its implications are substantive. Uncertainty about a document can become uncertainty about how to act. Even when the correct form is found, a business needs to know whether staff can complete it usefully. *"Do they put the right information on the document?"* he asked.

His proposed response was to rehearse the process through dummy reports as part of compliance monitoring. Employees should demonstrate that they can find the form, provide the relevant information and send it through the appropriate channel.

He drew a comparison with airline pilots: *"They simulate, they go through it."* For management, that approach offers evidence that a training record alone cannot provide. A simulated report can expose inaccessible documents, unclear instructions and incomplete information before those weaknesses affect a real concern.

The Chief Executive also cautioned against reproducing reporting diagrams without examining their substance. Discussing a diagram focused on suspicious activity, he observed: *"We also require reporting on knowledge."*

His point was that firms should ensure their internal materials reflect the scope of the reporting requirements he was discussing. A simplified illustration should not inadvertently narrow employees' understanding of what needs to be escalated.

AI AND THE INTERPRETATION OF SUSPICION

The same emphasis on testing ran through Beale's remarks on artificial intelligence. In his opening address, he referred to an apparent AI error involving his own identity and Jersey's regulatory role. The example illustrated a concern that would recur in his presentation: generated information can appear convincing while being wrong.

For firms using AI to process documents and examine client behaviour, the question is how reliably those tools recognise circumstances that warrant further attention.

A system may detect a predefined warning sign. Beale questioned whether it can also interpret the less explicit information from which suspicion can emerge, and whether it will prompt an appropriate escalation. *"It's not a human being,"* he reminded delegates.

His remarks acknowledged the usefulness of the technology while challenging firms to examine how their AI agents are instructed and tested. The adoption of automation leaves businesses needing to understand what triggers an alert, what information is passed on and how that information reaches the responsible officer.

Those questions connect technological investment with the organisational concerns that dominated his presentation. Both employees and automated systems operate within reporting arrangements whose effectiveness needs to be demonstrated.

Beale also argued for the use of case studies to examine behaviour and the risks of failing to recognise or escalate concerns. The focus was on whether firms could show that they were alert to the possibility of handling criminal proceeds, as well as on the subsequent reporting decision.

For businesses assessing their financial crime defences, his presentation suggested a concrete starting point: follow a concern from its first recognition to its eventual assessment. The exercise may reveal that the most consequential weakness lies before the formal reporting clock begins.

AMEER CAUNHYE, Chief Executive Officer of ACRION

“The next assessment provides an opportunity to demonstrate the results”

Mauritius has made substantial progress in strengthening its AML/CFT/CPF (Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing) architecture. But for Ameer Caunhye, the next challenge is more demanding as Mauritius needs to demonstrate effectiveness. Speaking to us at the 8th Financial Crime Conference on September 2, he stressed that, as the country prepares for its next assessment, compliance cannot be reduced to policies, procedures and statistics. What will matter is whether risk assessments translate into action, whether intelligence leads to investigations and prosecutions, and whether the different components of the system work together to deliver measurable outcomes.

You argue that compliance needs to move beyond box-ticking. Where is the traditional approach failing?

I think the traditional approach starts to fail when too much attention is placed on demonstrating that a compliance activity has been performed, rather than asking whether it has actually addressed the risk.

There is, of course, a need for policies, procedures, controls and proper documentation. I am certainly not suggesting otherwise. The difficulty arises when following the process becomes the objective in itself.

AML/CFT is fundamentally risk-based. That requires judgement. It requires people to understand why a control exists, recognise when something does not make sense, and be prepared to ask further questions rather than simply being satisfied that the prescribed process has been completed.

This becomes even more important in the digital age. Financial crime is evolving quickly. We are dealing with virtual assets, increasingly sophisticated fraud, artificial intelligence, synthetic identities and more complex cross-border transactions. A control that worked several years ago may still exist today, but that does not necessarily mean it remains effective today.

So, for me, moving beyond box-ticking is not about having fewer controls. It is about making sure those controls remain relevant to the risks and achieve the purpose for which they were designed.

What is the difference between being technically compliant and actually demonstrating AML/CFT effectiveness?

The distinction is perhaps clearest when we look at the way FATF assesses countries.

FATF has 40 Recommendations. Technical compliance assesses whether a country has put in place the necessary laws, regulations, institutions and other measures required by those Recommendations. But FATF deliberately has a second assessment: effectiveness. This is assessed through the 11 Immediate Outcomes, which look at whether the country’s AML/CFT/CPF system is actually delivering the results expected of it.

So, at national level, technical compliance might establish that Mauritius has the necessary legislation, supervisory authorities, Financial Intelligence Unit, investigative powers, preventive measures, beneficial ownership requirements and sanctions framework.

Effectiveness goes further. It looks at whether the country properly understands its money laundering, terrorist financing and proliferation financing risks; whether supervision is genuinely risk-based; whether preventive measures are being applied in practice; whether useful financial intelligence is being generated and used; whether money laundering and terrorist financing cases are being investigated and prosecuted appropriately; whether criminal proceeds are being identified and confiscated; whether legal persons are protected from misuse; and whether targeted financial sanctions relating to proliferation financing are operating effectively.

That is really the distinction I was trying to make at the conference: technical compliance tells us whether the architecture is there; effectiveness tells us whether the architecture is producing the intended results.

Mauritius has strengthened its laws and institutions considerably. How do we demonstrate that these measures are producing results?

Mauritius has made very significant progress on technical compliance. Today, Mauritius is Compliant or Largely Compliant with the 40 FATF Recommendations.

That is important because it means we have substantially strengthened the legal and regulatory foundations. The next challenge is demonstrating what those foundations are producing.

At national level, the key is to demonstrate a clear chain from risk identification to action, and from action to measurable outcomes.

Where a national or sectoral risk assessment identifies a material risk, that finding should translate into changes in policy, supervisory priorities and resource allocation. Supervisory programmes should be adjusted accordingly, with greater attention directed towards the areas of highest risk. That, in turn, should contribute to stronger detection, better-quality financial intelligence, more targeted investigations and, where appropriate, prosecutions, asset restraint and confiscation.

The important point is that the risk assessment should not end with the identification of risk; it should visibly influence what the system does and the results it produces.

It is the connection between those different parts of the system that matters.

FATF’s effectiveness methodology is built around that concept. The 11 Immediate Outcomes do not simply ask what a country has put in place. They look at whether the different parts of the AML/CFT/CPF system are producing the intended results.

So, I think that Mauritius needs to be able to tell a coherent, evidence-based story: these were our principal risks; these were the measures we took in response; and these are the results those measures produced.

In an effectiveness assessment, what evidence matters most to international assessors?

FATF’s Assessment Methodology is very useful on this point because effectiveness is not assessed simply by counting activities.

The methodology requires assessors to determine the extent to which each of the Immediate Outcomes is being achieved, taking into account the country’s risks, context and materiality. FATF’s revised methodology also places greater emphasis on the major risks facing the country, so that good results in lower-risk areas do not distract from weaknesses in areas that really matter.

Assessors will therefore look at both quantitative

Cont’d on page 19

and qualitative evidence.
Statistics are important: inspections, sanctions, STRs, investigations, prosecutions, convictions, confiscations, international cooperation and other measurable outcomes. But numbers need context.

For example, a large number of STRs does not by itself demonstrate effectiveness. Assessors will want to understand their quality, whether they reflect the country's risk profile, whether they generate useful financial intelligence and whether that intelligence is actually used.

The same applies to supervision. The number of inspections matters less if supervisory resources are not being directed towards the sectors and institutions presenting the greatest risks.

Case studies are therefore extremely valuable because they allow Mauritius to demonstrate how the system worked in practice.

Where do you see the greatest risk of Mauritius having good frameworks on paper but insufficient effectiveness in practice?

At national level, I think one of the main risks is a disconnect between the different components of the system.

Mauritius can have strong legislation, competent authorities, national strategies, risk assessments and sophisticated regulatory requirements, but effectiveness depends on how all those elements work together.

For example, identifying a national risk is only the beginning. That risk needs to influence policy, supervisory priorities, resource allocation, financial intelligence, investigations, enforcement and, ultimately, outcomes.

There is also the question of feedback. What are supervisors learning from inspections? What is the FIU learning from STRs? What are law-enforcement agencies learning from investigations? What are prosecutors learning from cases that do or do not succeed? Are those lessons feeding back into national risk assessments, guidance, supervisory priorities and private-sector controls?

FATF specifically says that the objective of an effective system can only be achieved when the different components of a country's AML/CFT framework are operating well together.

So, for me, the greatest risk is not necessarily that one component is missing. It is that all the components exist, but the connections between them are not strong enough to produce the desired outcome.

Is the private sector sufficiently prepared for this shift from compliance to measurable outcomes?

There has undoubtedly been a significant increase in AML/CFT awareness and capability within the Mauritian private sector, particularly following the experience of the FATF grey list. But I think proliferation financing illustrates one of the challenges we now face.

Mauritius completed its second national Money Laundering and Terrorist Financing Risk Assessment in 2025. However, the country's first National Proliferation Financing Risk Assessment is still being undertaken. The National AML/CFT/CPF Strategy 2026–2029 itself confirms this.

At the same time, the legislative framework has evolved and reporting persons are now required to assess and mitigate proliferation financing risks.

That creates a practical challenge. A proper risk-based approach should be informed by the national understanding of risk. Reporting persons are being asked to assess their own exposure to PF at a time when the national PF risk assessment that should provide an important source of context is still being developed.

That does not mean reporting persons should wait. There are other sources available: FATF guidance and typologies, sanctions information, supervisory guidance, international PF cases, geographic and sectoral risk indicators and the reporting person's own customer, product and transaction exposure.

But it does illustrate why national and private-sector preparedness have to move together. Once the national PF risk assessment is completed, it will be important for its findings to be disseminated effectively and translated into practical sectoral guidance so that reporting persons can revisit their own assessments and controls against a clearer national picture.

This is a very good example of the difference between introducing a requirement and ensuring that the wider ecosystem exists for that requirement to operate effectively.

What lessons should Mauritius draw from jurisdictions that have struggled with effectiveness assessments?

I think Mauritius should first look at its own previous assessment.

I have read the 2018 Mutual Evaluation ratings because they provide an important benchmark. Mauritius received Low effectiveness ratings for seven of the 11 Immediate Outcomes and Moderate effectiveness ratings for the other four. There were no Substantial or High effectiveness ratings.

That assessment was based on the position at the time of the on-site visit in 2017 and Mauritius has changed considerably since then. We subsequently made very significant progress, particularly on technical compliance. But the previous results still contain an important lesson.

It is possible to improve laws, regulations and institutional arrangements considerably while still having to demonstrate that the system produces results.

This is not unique to Mauritius. FATF's global experience shows that effectiveness has generally been more difficult for countries to demonstrate than technical compliance.

The second lesson is that preparation cannot simply be an exercise undertaken shortly before assessors arrive. FATF's methodology looks at outcomes and evidence. Those outcomes have to develop over time.

The third lesson is to focus on our material risks. The revised FATF methodology places greater emphasis on whether countries are achieving results in the areas where their risks are highest. It is therefore not enough to demonstrate that the system works somewhere; Mauritius needs to demonstrate that it works where it matters most.

For me, the lesson is quite simple: do not prepare merely for the assessment. Use the assessment as an opportunity to strengthen the system.

If you had to identify three priorities for Mauritius before its next assessment, what would they be?

My first priority would be to maintain a current understanding of our national risks and ensure that this translates into action. Risk assessments should inform policy, supervisory priorities, resource allocation and private-sector controls. The ongoing National Proliferation Financing Risk Assessment is one example of how Mauritius is continuing to strengthen its understanding of evolving risks.

My second priority would be to strengthen the evidence of effectiveness across the 11 Immediate Outcomes. Mauritius should be able to demonstrate, through reliable data and practical case studies, the results being achieved across supervision, financial intelligence, investigations, prosecutions, confiscation, international cooperation and other key areas. The focus should increasingly be on outcomes rather than activities alone.

My third priority would be to strengthen coordination across the entire AML/CFT/CPF ecosystem. Effectiveness depends on policymakers, supervisors, the FIU, law enforcement, prosecutors and the private sector working together, sharing relevant information and ensuring that lessons from one part of the system inform the others.

Mauritius has already made considerable progress in strengthening its legal, regulatory and institutional framework. The next assessment provides an opportunity to build on that progress and demonstrate the results being achieved in practice.

The next chapter for Mauritius is not about starting again; it is about demonstrating the effectiveness of what we have built.

ANDY JARVIS, Co-Founder and Chief Digital Officer of Elevated eXperience

"Legacy systems are leaving the door open to financial crimes"

Mauritius has the connectivity, talent and digital ecosystem to strengthen its defence against financial crime. But according to Andy Jarvis, the country's financial-services sector must stop layering new technology onto outdated infrastructure. His warning is stark: fragmented systems, spreadsheets and paper-based processes create gaps that criminals can exploit, while AI can make those weaknesses even more dangerous. "AI does not automatically fix bad systems. It can simply make bad processes faster," says Andy Jarvis. Speaking at the 8th Financial Crime Conference at Hilton Resort & Spa on September 2 and 3, he urged the country's financial-services sector to accelerate its digital transformation, eliminate paper-based processes and develop a new technology infrastructure rather than continually extending legacy systems.

You argue that broken and disconnected systems are a gift to financial criminals. How exactly do criminals exploit those gaps?

It is a mixture of things. I work with institutions, enterprises and corporates of varying sizes, from small to large. One of the fundamental problems is that technology grows over time. You start with a system, then you build and build and build. You might begin with a trust and company service provider system or a banking platform such as T24, and then layer more technology on top.

What happens is that, over time, staff come and go. People are not necessarily trained properly; they are often trained by the person who is leaving. So, you have complexity and gaps in education. And therefore, you have gaps in the process. That is where criminals come in and exploit those gaps.

The other thing that happens is that the world's most loved system is Excel. If people want to work with data, they export it to Excel. Every system in the world seems to have an *"export to Excel"* button.

The minute you dump information into Excel, it is not encrypted, it is not audited, it is not backed up, and the IT department often does not know anything about it. That is where crime happens because the data is essentially open to interpretation.

Are financial institutions investing heavily in new technology while still operating with fundamentally fragmented systems?

Yes indeed. I think one of the biggest things to answer that question is that no one ever turns anything off.

There is a lack of investment in consolidating what you have today and making the best of what you already have. Instead, there is a real willingness to invest in the next best thing because competitors are doing it or customers are asking for the latest innovation.

Are we implementing a chatbot on our website? Are we implementing AI in our systems? In fact, crime can happen silently in our organisations. Sometimes it happens from within; sometimes externally. And the channels are everywhere.

Currently, the cost of simply maintaining compliance in our organisations is around USD 206 million a year globally, and that is before any financial crime happens. That is just trying to keep the back door shut and it is still wide open. It is effectively a tax: a subscription that none of us signed up for, a bit like Spotify.

Where is the greatest vulnerability today? Outdated technology, poor data sharing, human error, or organisations working in silos?

Probably, well, all of the above. But the biggest vulnerability is human error. That does not mean people go to work intending to make mistakes. The problem is that the processes have become increasingly complicated, with numerous workarounds, manual interventions and spreadsheets embedded in organisations.

Take, for example, the Barings Bank incident where the bank lost more than USD 800 million. Essentially, a securities trader was managing investments through a spreadsheet and made a simple copy and paste error. A calculation that was supposed to average figures ended up summing them instead.

The consequences were enormous!

Mistakes happen every day. But when those mistakes occur within complex financial systems, the value and impact of a seemingly small human error can be massive.

Can you give us an example of how a seemingly minor disconnect between two systems can create an opportunity for financial crime?

I think one of the biggest ones, again, is within the compliance function itself - anti-money laundering and KYC. The majority of the organisations that I work with run those functions on spreadsheets.

So, the disconnect between systems is fundamentally that the work is not being done in a system; it ends up in a system after the compliance work has been done.

So, you are extracting things from a system to run a set of processes on spreadsheets, or on paper, or you are emailing files backwards and forwards. And the intersection for a criminal has nothing to do with the systems.

The systems are controlled, but you are working outside them. And that is where the gap is. Unbelievable.

We are still making the same mistakes we were making 20 years ago!

Financial institutions collect an enormous amount of KYC and transaction data. Is the real problem now, not the lack of data, but the inability to connect and interpret it effectively?

Exactly. KYC data is often captured outside core systems, so the ability to genuinely verify it is limited.

Firms are now implementing KYC and KYB platforms that can do things such as automated passport scanning. But they are still open to human interpretation.

But they are still open to human interpretation. And equally, you have insider attacks. People can override controls quite easily. Everything is still subject to fraud. We hear cases every day about fraudulent copies of passports circulating and people being hacked all the time.

It is not a bomb-proof science. My concern is that you then put AI on top of that and take away some of the human intervention or intelligence needed to interpret something through multiple checkpoints.

AI is essentially giving you an answer, and that answer is not always correct. You could therefore end up taking on a business or transacting business that you do not necessarily want to be doing.

As criminals increasingly use AI and automation, are banks and compliance teams technologically equipped to keep pace?

No. I mean, I could leave it at that. Take a

Cont'd on page 21

very good example. A lot of banks are now implementing WhatsApp as a customer communication channel. At the same time, criminals are literally building farms that use WhatsApp to harvest credentials and then hack accounts.

The South African government, as a really good example, is using WhatsApp as a primary communication channel now. And it has been proven that this is a weak backdoor. WhatsApp Business is, yes, perhaps encrypted, but it is not a secure channel because it does not have the verification mechanisms required.

All you are essentially verifying is: does my client have this phone number? Yes. But that is not an unhackable route.

Could AI actually create another layer of risk if institutions integrate it into already fragmented or poorly designed systems?

Absolutely.

Within an organisation, the technology stack is generally looked after by the IT team. They manage the banking platform and the core systems. But they are often unaware of the spreadsheets, the data sitting in SharePoint and all the other places where information actually resides. The real working processes are largely understood by the staff, not the IT teams.

Then the IT teams implement AI for employees to use, without necessarily knowing how that AI is actually being used. So, AI is going to accelerate it.

On an unstructured dataset, AI will essentially give you the same answer — if not worse — in a faster time, with better grammar, wearing a nicer suit. It is essentially accelerating the car crash.

If you do not get rid of the legacy and the complexity, the car will eventually crash. You put AI on top of that and you simply speed it up.

How do institutions modernise legacy systems without creating new vulnerabilities during the transition?

When we work with an organisation, the primary thing we focus on is making sure that, at board level and within the leadership and management teams, everyone has one vision, one set of values and one mission.

Organisations today often do not. At best, you have three different directions.

You have the technology function, which has its own strategy, vision, mission and budget. Then you have the people function, which is focused on employees and protecting the organisation. And then you have the client-facing teams — sales and marketing — dealing with customers and operating according to another strategy.

They utilise IT, but those three groups do not necessarily talk to each other. We bring them together and make sure they are aligned. They need the same mission, the same roadmap and the same transformation plan.

You cannot stop vulnerabilities from creeping in. What you can do is agree on getting to a better future, establish the timeline and create a roadmap.

We give teams a 30, 60 and 90-day plan to resolve immediate issues.

But my advice is simple: turn off as much of the old stuff as you can, as fast as possible.

Mauritius is an international financial centre connecting Africa, Asia, and Europe. Does that interconnectedness make system integration and real-time information sharing even more important?

Absolutely. A really good example is where I come from. In Jersey, we worked for years to build connectivity. I worked in telecoms for quite a long time, including on the world's first fully fibre network.

Mauritius is now in a really strong position from a connectivity perspective. Despite reliability issues around power and infrastructure, you are one-gigabit connected. And the interconnections between Mauritius, India and Asia are extremely powerful. I think it is still early days, but you are in a very strong position as an island nation.
You are self-governed, you have a well-educated population and a strong expatriate population. You are consuming global knowledge. Your ability to connect not only to India and Africa, but globally, puts you in a strong position to close the door on financial crime.

Mauritius has already demonstrated that it can respond quickly when it decides to act. The country was placed on the FATF Grey List and subsequently, 18 months later, removed after addressing the identified deficiencies.

That is a very good example of the government saying: "We have these issues; we are going to close every single one of them."

If institutions follow the same approach, the world will be a much better place.

So, if you were advising the Mauritian financial services sector, what is the one technological or organisational weakness that you would address first?

I think, the number one, after looking at the landscape here, is: "Get off paper".

There are still a lot of paper processes here. There is still significant reliance on people physically coming into an office with documents. Given the way the world is moving, particularly with AI and the acceleration of financial institutions globally, there is a real danger of being left behind because other international financial centres will move faster.

And where you have paper, you have opportunities for crime. Where you have digital systems, you lessen those opportunities. As an island nation, Mauritius can also be quite nimble in implementing technology.

You have a good digital ecosystem and a strong digital sector. We have been talking to people in South Africa who have literally moved to Mauritius because of the investments being made in digital technology. Take that and utilise it faster. But again, turn the old stuff off as quickly as possible.

I was speaking to someone from a large banking institution and he asked me what I would do. I said: "Build the new house. Operate like a startup."

What do you actually want to do? Forget the history. Forget the legacy. Your existing clients may be perfectly happy with the systems they have been using for 20 years. But that is not the point. The question is: what do you want to do as an organisation, and how do you avoid being left behind by the startups coming after you?

Big institutions can fail very quickly. Look at Blockbuster. It went bankrupt because it did not see streaming coming. It thought it would never take off. If an institution believes it cannot build a new infrastructure and gradually move its clients into it, it is wrong. It will ultimately fail.

So, the imperative is - and I will reiterate this strongly – to invest in getting off your legacy.

What do conferences like the 8th Financial Crime Conference, held at Hilton Mauritius Resort & Spa on 02 and 03 September 2026, contribute?

I think it's the can-do attitude. So, for the suppliers like us, it is about bringing global knowledge to a local table. The way my business operates, I am a keynote speaker first. Then we run masterclasses and work with leadership teams, empowering them with tools, techniques and know-how. But we also work with local partners.

We are a small operation, but we have partners all over the world. Coming to Mauritius is therefore about building that network and developing strong partnerships. We can leave knowing that the local market is in good hands because people have learned something and are using frameworks that are accredited by us and proven to work.

For attendees, I think it is about getting out of your day job for a couple of days and having the opportunity to think clearly about what you are actually doing. How many times in an organisation are you sitting there pushing buttons and filling things in without really knowing why?

You are taught to fill in the form and tick the box. Then, when something happens whether it is a disaster, an anomaly or a criminal event, it can be difficult to spot because you do not understand the mechanics behind it.

The best drivers in the world are often very good mechanics because they understand how the car works. You can get into a car and drive it fast, but only up to a point. That is why Lewis Hamilton has won seven world championships. He can talk to the team and say, "I need that front wing," because he understands exactly what changing it will do.

There are not many people in organisations with that level of know-how.
So, I would strongly encourage people to learn, learn, learn and question everything. That is how you help your organisation truly thrive.

SANJANA KISSOONDHARRY, Head of Financial Crime Compliance / MLRO – Absa Bank Mauritius

"Combat technology with technology"

As artificial intelligence, deepfakes and behavioural analytics reshape the financial crime landscape, banks can no longer rely on yesterday's risk models. Sanjana Kissoondharry, Head of Financial Crime Compliance / MLRO at Absa Bank Mauritius, says criminals are exploiting technology to operate faster, at a greater scale and with unprecedented sophistication. Yet she argues that technology alone is not the answer: the future of compliance lies in combining advanced analytics with human judgement, skilled professionals and a genuinely risk-based approach: "Whether it is AI-driven transaction monitoring, behavioural analytics or automated compliance processes, the human being remains central to making informed, proportionate decisions."

What financial crime threats are banks seeing today that were far less significant five years ago?

If we look back 5 years, banks were concerned with the traditional financial crime typologies, including fraud, identity theft, social engineering, and money mule activity. These typologies still exist today, but the channels through which these financial crimes are happening have changed.

New technologies, including artificial intelligence, robotic automation tools and blockchain technology, are being actively used by criminals to perpetrate frauds, scams and similar criminal activities. Examples include using artificial intelligence technology to create deepfakes for investment scams, or using the same technology to create synthetic identities that can be used for account opening.

The underlying objectives have not changed – that is, generating proceeds from financial crime activities. What has changed is that technology is allowing criminal activities to be conducted faster, at a greater scale and with a higher degree of sophistication. All of this is happening without geographical constraints. Financial crime remains a worldwide phenomenon.

How are AI, deepfakes and sophisticated digital fraud changing banks' risk models?

In relation to the banking sector, the impact is twofold. Firstly, banks are themselves increasingly becoming targets of technology-enabled fraud. Criminals are using AI and deepfakes to create sophisticated and realistic impersonations. Criminals have been using tactics to persuade customers to transfer funds or disclose credentials such as passwords. These new technology-enabled methods have just made it easier and faster.

Secondly, banks are at the centre of these ecosystems, where banking products can be abused by criminals to facilitate the movement, layering and integration of proceeds from these criminal activities.

It is therefore no longer sufficient to rely on historical models that have not evolved to include new technologies. The risk assessment models have to continuously evolve and be updated to ensure that they encapsulate emerging threats and new technology risks, both from a financial crime risk perspective and a technology adoption perspective. From there, institutions will have a better understanding of what risks they are exposed to and what controls are necessary to remain within their risk appetite.

Investment in technology, controls and people through extensive training is crucial to adapt to this future of financial crime. Combat technology with technology.

How do banks distinguish genuinely suspicious behaviour from unusual but legitimate customer activity?

Banks do not automatically treat unusual activity as suspicious activity. Rather, they use a risk-based approach to determine whether there is a legitimate explanation for the behaviour before concluding that it may be indicative of financial crime.

In practice, banks distinguish the two by looking at the customer's known profile and expected behaviour. Transactions are assessed against what is known about the customer's occupation, business activities, source of wealth, source of funds, historical transaction patterns, and expected account usage. Activity that deviates from this profile may be unusual, but not necessarily suspicious.

The availability of a reasonable explanation: an unusual transaction often has a legitimate rationale. For example, a large deposit may result from the sale of a property, the maturity of an investment, or receipt of an insurance payout. Where the customer can provide a credible explanation supported by documentation, the activity may be considered unusual but legitimate.

Patterns rather than isolated events: banks focus on transaction behaviour over time. Repeated inconsistencies, rapid movement of funds,

Cont'd on page 23

unexplained third-party payments, transactions that lack an apparent economic purpose, or activity inconsistent with the customer's profile are more likely to give rise to suspicion.

The presence of red flags: suspicion generally arises where there are indicators suggesting potential money laundering, terrorist financing, fraud, or other illicit activity. Examples include structuring transactions to avoid reporting thresholds, unexplained use of third parties, activity involving high-risk jurisdictions, or customers providing false, vague, or inconsistent information.

Increasingly, technology plays a critical role in improving the accuracy and effectiveness of this process. Advanced transaction monitoring systems, analytics, network analysis, and AI-driven models enable banks to analyse vast volumes of customer activity, identify patterns that may not be apparent through manual reviews, and establish more accurate behavioural baselines for individual customers. This helps reduce false positives, improves the quality of alerts generated, and allows investigators to focus their efforts on genuinely higher-risk activity.

However, technology alone is not sufficient. Effective financial crime risk management continues to rely on a human-in-the-loop approach.

While systems can identify anomalies and generate alerts, experienced investigators and relationship teams apply judgement, assess context, consider customer explanations and supporting documentation, and determine whether the activity is genuinely suspicious or simply unusual but legitimate.

The combination of advanced technology and informed human judgement enables banks to achieve more accurate outcomes, strengthen financial crime detection, and ensure that legitimate customers are not unnecessarily inconvenienced.

Is there a danger of banks becoming excessively risk-averse because of regulatory pressure?

There is certainly a risk that banks may become overly cautious in response to an increasingly complex risk and regulatory environment. With the emergence of new financial crime risks, heightened regulatory expectations, and the need to maintain robust customer due diligence and ongoing monitoring frameworks, banks are required to make significant investments in compliance, controls, and risk management.

Both globally and locally, we have seen instances of de-risking, where certain customer segments, industries, or relationships have been exited because the perceived risks and compliance costs outweighed the commercial benefits. While these decisions are often made with the intention of protecting the institution, they can give rise to unintended consequences.

One of the most significant consequences is the potential impact on financial inclusion. Overly restrictive AML/CFT controls can unintentionally exclude legitimate customers from the formal financial system, driving greater reliance on cash transactions, informal channels, and unregulated networks, which may ultimately undermine the very objectives that financial crime controls seek to achieve.

Importantly, global standard setters have long recognised this challenge. FATF has consistently emphasised that financial inclusion and AML/CFT objectives are complementary rather than competing goals. Similarly, the Bank of Mauritius has recently enhanced its guidelines to support the application of simplified measures in circumstances where risks can be demonstrated to be lower, reinforcing the importance of proportionality in the application of controls.

The solution is therefore not to eliminate risk, but to manage it intelligently. Effective risk management requires a genuine risk-based approach that differentiates between higher and lower-risk customers, products, and activities. Rather than relying on blanket exclusions or broad de-risking exercises, banks should leverage quality data, technology, and informed human judgement to assess customers individually and apply controls that are commensurate with the risks presented.

Ultimately, the most successful institutions will not be those that avoid risk altogether, but those that are able to manage risk confidently, support financial inclusion, and enable economic activity while continuing to meet their regulatory obligations.

How do you reconcile increasingly stringent KYC requirements with customers' expectations for faster banking services?

Strong KYC controls and a good customer experience are not mutually exclusive when the right foundations are in place.

First, our people must have a clear understanding of regulatory requirements and the confidence to make timely, risk-based decisions, escalating matters where appropriate.

Second, processes should be streamlined, with clear accountability and the removal of unnecessary governance layers that create delays. These processes should be regularly reviewed to ensure they remain efficient and fit for purpose.

Third, technology can play a critical role by automating routine activities, leveraging advanced analytics, and integrating trusted data sources to enable faster, risk-based onboarding and ongoing monitoring. This not only improves efficiency but also enhances the quality and consistency of decision-making.

Importantly, we must also view this through the lens of the customer. Customers rightly expect banking services that are simple, seamless, and delivered with speed. However, there must also be an appreciation that banks operate within a highly regulated environment and have a responsibility to comply with legal and regulatory requirements designed to protect the integrity of the financial system. Effective KYC, customer due diligence, and ongoing monitoring are therefore not administrative hurdles, but essential safeguards against financial crime, fraud, and abuse of the financial system.

The objective is not to choose between compliance and customer experience, but to strike the right balance. By combining well-trained colleagues, efficient processes, intelligent use of technology, and proportionate risk-based controls, banks can meet their regulatory obligations while delivering a customer experience that is both frictionless and trustworthy.

Can AI materially reduce false positives in transaction monitoring?

Yes, I do believe that technology has the potential to reduce false positives in transaction monitoring.

A number of third-party vendors are offering AI-powered solutions that can be integrated into existing transaction monitoring systems. These tools provide an additional layer of analysis before escalation for human review. Many of these solutions are designed specifically to improve alert quality, and they can be helpful in freeing up resources to focus on higher-risk cases.

That said, my view is that financial institutions should adopt these technologies with caution. Before implementation, it is important to ensure that the solution is compatible with existing systems and operational processes. In addition, AI models can be susceptible to bias and hallucinations, particularly when decisions are based on incomplete or poor-quality data. For this reason, human oversight and human judgement remain essential. We should keep human in the loop, especially where compliance decisions and regulatory obligations are concerned.

More significantly, the shift from traditional rule-based monitoring to behavioural monitoring, facilitated by new technologies, can be more disruptive. Traditional systems, relying on thresholds and predefined rules, can generate false positives as well as false negatives. Behavioural monitoring, on the other hand, can continuously assess activity against patterns, using broader set of indicators, such as geolocation, device behaviour, network connections and document authenticity against customer profile. I believe that a combination of traditional rule-based monitoring and behavioural analytics using new technologies provides stronger tools for detecting indicators of financial crime, especially when the emerging risks we are seeing are harder to detect.

Eventually, the value is in intelligent predictive monitoring.

Will the compliance function of the future require more technologists and data specialists than traditional compliance professionals?

The compliance function of the future is actually now.

There should be a combination of traditional compliance professionals working alongside technologists and data specialists. The compliance function model has to be revised deliberately.

Additionally, compliance professionals should be investing now in developing their knowledge and expertise on these new technologies, whether it is AI-driven or blockchain-based. At the same time, compliance professionals must have a strong understanding of the risks these technologies bring to the environment, whether from a financial crime or regulatory perspective. Therefore, the compliance function should be made up of a blend of skills and backgrounds. This will help organisations improve existing traditional approach and to design more effective controls to cater for these emerging concerns.

Importantly, the compliance function can be complemented with AI tools and automation, with repetitive, low-risk tasks being automated with a human in the loop. This will allow compliance professionals to focus on the higher-risk areas.

Compliance professionals are not becoming less relevant; rather, their role is becoming increasingly strategic. Realising this potential will require organisations to invest deliberately in elevating the compliance function beyond its traditional oversight mandate, positioning it both as a strong risk guardrail and as a trusted partner that enables sustainable business growth.

TAWHEEN CHOOMKA, Legal Practitioner & Founder - LexCorp Chambers & Lexcorp Training Institute

"Waqf was unfamiliar 15 years ago, and I would say that it remains unfamiliar today"

On the second day of the eighth Financial Crime Conference at Hilton Mauritius Resort and Spa on September 3, legal practitioner Tawheen Choomka said the country's 2026 waqf reforms would subject Islamic endowments to stricter registration, beneficial ownership and AML/CFT controls. The measures are intended to prevent charitable donations and digital cross-border payments from financing terrorism and proliferation.

Mauritius has brought waqf structures under a more demanding anti-money laundering and counter-terrorist financing regime, seeking to modernise oversight of an institution governed by legislation dating from 1941.

The reforms make registration compulsory, require beneficial ownership records and transform the Board of Waqf Commissioners from a largely administrative institution into an investigative, regulatory and supervisory authority. Financial auditors are also expected to report suspicious transactions, while breaches of the new compliance duties may attract fines of up to Rs 1 million.

Tawheen Choomka, a legal practitioner and founder of LexCorp Chambers and Lexcorp Training Institute, said the amendments had awakened a structure that remained poorly understood in Mauritius despite its long history and extensive use overseas.

"Waqf is very dear to me because it is a sleeping beauty," she said. *"The law governing waqf in Mauritius dates from 1941. Since then, the structure has largely been overlooked."*

Tawheen Choomka spoke on September 3 during the second day of the eighth Financial Crime Conference, held at the Hilton Mauritius Resort and Spa. Her session, "*The Future of Waqf Governance: Navigating AML/CFT Compliance in the Digital Age*", formed part of a programme covering national co-ordination, sanctions, artificial intelligence, banking controls, real estate, asset tracking and changing financial crime risks across Africa.

The conference was organised by the Academy of International Finance in partnership with Comsure Compliance and brought together regulators, prosecutors, lawyers and industry specialists on September 2 and 3. Its theme was *"Financial Crime Prevention and Detection in the Digital Age"*.

AN UNFAMILIAR STRUCTURE

A waqf is a permanent dedication of property whose use or income is generally applied to religious, pious or charitable purposes. An owner, known as the waqif, dedicates an asset through a document called a waqf-nama and appoints a mutawalli to manage it.

There are broadly two forms. A family waqf can hold property for the benefit of children or other family members. A charitable waqf receives, manages and distributes assets or income for a specified public, religious or philanthropic purpose.

The arrangement resembles a trust, but it is legally distinct. Trusts are supervised by the Financial Services Commission, while waqf structures fall under the Board of Waqf Commissioners and the Waqf Act 1941. Mauritius enacted its Trusts Act only in 2001, six decades after the waqf legislation, although financial professionals typically explain waqf by comparing it with the more familiar trust.

Tawheen Choomka said the lack of familiarity had practical consequences. She recalled receiving her first corporate assignment after being admitted to the Bar at the age of 22. The client, the founder of a Mauritius waqf living in France, suspected that the mutawalli had been siphoning money from several bank accounts.

The waqf-nama, an old handwritten deed, stipulated that the structure should maintain only one account. The existence of several accounts was therefore a clear breach. The mutawalli was the sole signatory, withdrew money

Cont'd on page 25

and provided no justification for payments, while the founder did not know what was happening and could not travel repeatedly to Mauritius.

She obtained a power of attorney and approached the bank to close the unauthorised accounts and transfer the balances into the remaining account. Bank staff struggled to classify the customer.

"'What type of structure is it?'" she recalled an officer asking. *"I said it was a waqf. He asked whether it was a société. I said no. He asked whether it was a company. Again, I said it was a waqf."*

"Nobody understood what a waqf was," she said. "The concept was unfamiliar 15 years ago, and I would say that it remains unfamiliar today."

The structure is more widely recognised in jurisdictions including Singapore, Malaysia, Saudi Arabia and the United Arab Emirates. In Mauritius, however, management companies rarely administer waqf structures and banks may have limited experience dealing with them.

The legal practitioner argued that this gap could represent a new line of business for banks and management companies. Waqf structures were traditionally associated with real estate, but clients are now considering the structure for company shares and intellectual property. Consumable property is the principal exception; other forms of property can generally be dedicated to a waqf.

"Waqf is nevertheless becoming more important and popular," she said. *"With an AML/CFT framework now in place, more people may consider waqf alongside trusts and foundations."*

GREY-LIST LEGACY

The push for stronger controls has its roots in Mauritius's placement on the Financial Action Task Force grey list in 2020. "The sleeping beauty was kissed, not by a prince but by the grey list," Choomka said. "That woke us up, and we decided to change the compliance framework for waqf."

The principal concern is not the structure itself but the financial flows that some charitable waqf receive and distribute. A waqf may hold a property, collect its income and transfer part of the proceeds to an international charity. The payment may appear consistent with the waqf's stated purpose, while the receiving organisation could in fact have links to terrorism or proliferation financing.

Modern fundraising has magnified the risk. Donations can now be solicited through social media and received instantly through QR codes, bank transfers, payment platforms or virtual assets. Money may arrive from several countries, pass through intermediaries and then be sent overseas to build a school or provide humanitarian aid.

An invoice received by email does not necessarily prove that funds reached their intended destination.

"Can anyone guarantee that the money will be used for the stated purpose?" she asked. *"Who verified the donor and recipient? Who authorised the transaction? Were the recipients screened? Who controls the overseas organisation?"*

A waqf may also need to identify co-ordinated donations, detect the proceeds of cybercrime and preserve an audit trail covering five or six years. Individually small payments can create significant exposure when they are aggregated.

"Materiality is not relevant to terrorist financing or proliferation financing," Tawheen Choomka said. *"A contribution may be only Rs 100, but it can be pooled with other funds and used to finance terrorism or proliferation."*

She referred to a separate corruption case involving Rs 100 in which the offender received a three-year prison sentence, illustrating that a modest amount did not remove criminal liability.

The new framework consequently emphasises identity, traceability, governance, digital resilience and risk-based oversight. Donors and recipients must be understood, international beneficiaries screened and transactions supported by reliable records.

"The objective of regulation should not be to regard charity with suspicion," she said. *"It should make donors consider the risks when sending money abroad through a charitable waqf."*

A TRANSFORMED REGULATOR

The Board of Waqf Commissioners is now positioned alongside authorities such as the Financial Services Commission, Financial Intelligence Unit, Financial Crimes Commission and Registrar of Companies.

It can request information and documents, conduct inquiries and investigate suspected breaches. Under the amendments, the Board may delegate a commissioner or another person to enter premises and ask questions. Refusal or failure to answer can constitute an offence punishable by a fine or imprisonment.

Members of the Board are expected to understand both Islamic law and compliance law — a combination that may prove difficult to assemble in practice.

The legal practitioner also questioned the institutional design. The Board is chaired by a Supreme Court judge, but its enlarged remit includes investigative functions.

"Are judges equipped to conduct investigations?" she asked. *"My personal view is no: judges are not investigators."*

The reforms should also be viewed within a wider regulatory system in which several institutions may have overlapping responsibilities. Choomka said compliance professionals sometimes received different answers to the same question from different regulators.

"Our regulatory institutions do not always work together towards a single goal," she said. *"We lack sufficient collaboration between them."*

Effective implementation would require goal congruence and sustained information-sharing among the relevant authorities. Without it, organisations could face inconsistent expectations and uncertainty over which regulator's interpretation should prevail.

AUDITORS FACE UNANSWERED QUESTIONS

The legislation gives financial auditors an obligation to report suspicious transactions and file suspicious transaction reports. Choomka, who is also ACCA-qualified, said the provision raised questions about the relationship between the waqf amendments, the Financial Reporting Act and the existing definition of prescribed activities.

Auditors generally examine records, test samples and request explanations. Artificial intelligence may eventually allow them to examine every transaction, but much audit work remains sample-based.

The question is whether an auditor working for a waqf is performing a prescribed activity that triggers a formal reporting duty. The Financial Reporting Act does not appear to contain a corresponding provision, Choomka said.

Lawyers face a similar distinction. Providing legal advice alone may not trigger the full range of compliance obligations. Incorporating companies, acting as a promoter or secretary, or carrying out activities under a corporate services licence can bring the practitioner within the regulated perimeter.

"The 2026 regulations may therefore be only the tip of the iceberg," she said. Definitions and obligations may need to be refined as the framework develops.

Another potential anomaly concerns the levy paid to the Board. Every Mauritius waqf must contribute about 2.5 per cent of its gross annual income to the supervisory body. Choomka questioned what should happen if the income had an illicit source and a share of it was paid to the regulator responsible for overseeing the structure.

"There are many grey areas. "The reform is a strong start, she added, but some provisions warranted further debate."

BURDEN ON SMALL WAQF

The central challenge is how to impose effective controls without making legitimate charitable work unmanageable.

Under the 1941 Act, a mutawalli does not have to possess professional qualifications. The manager may be a friend of the founder, have limited education or training and manage only a small portfolio of property. Such an individual may now be expected to identify beneficial owners, screen transactions, understand terrorist-financing risks, maintain records and respond to a regulator.

"*How can such a person manage real estate and meet the new AML/CFT obligations?"* Choomka asked. *"It is extremely difficult without access to tools such as compliance software."*

A paper-based system is unlikely to provide the monitoring, screening and traceability required for modern cross-border transactions. Digital platforms, cyber-security controls, data-protection safeguards and artificial intelligence could help waqf managers meet the new demands.

Choomka said technology could also release professionals from repetitive compliance work and allow them to devote more attention to strategy. Making compliance easier through software did not weaken a compliance culture; it could strengthen it.

The regulatory response nevertheless had to remain risk based. Imposing identical paperwork on a small family endowment and a large charitable waqf receiving international donations would not necessarily deliver effective supervision.

Compliance had to be balanced with commercial or charitable purposes, Choomka said. Allowing business considerations to override compliance could result in sanctions and unfair practices, but allowing compliance to displace the organisation's purpose would also be damaging.

PENALTIES SIGNAL A CHANGE IN PRIORITIES

The amendments create a stark divide between older offences and failures under the modern compliance regime.

Certain breaches of the original Waqf Act still carry fines of only Rs 500. By contrast, a failure to meet the new AML/CFT requirements may result in a fine of up to Rs 1 million. *"A mutawalli who breached a traditional duty might face a fine of only Rs 500, while a failure to fulfil compliance duties can now attract a much larger penalty,"* Choomka said.

The difference reflects how far financial crime regulation has moved beyond the concerns of the 1941 statute. The institution may be centuries old, but it now operates through digital banking, online donations, international transfers and potentially virtual assets.

Mauritius has accordingly established a more comprehensive framework covering registration, beneficial ownership, suspicious activity and regulatory investigation. Its success will depend on whether the Board has the expertise and resources to exercise its powers, whether auditors and other professionals receive clear guidance, and whether regulators can work together.

For the financial services industry, the reforms present both an obligation and an opportunity. Banks, management companies, lawyers and compliance providers will need to understand a structure many have rarely encountered. They may also find demand for professional administration, governance and technology services as waqf become more diverse.

"Waqf is another structure for financial services professionals to understand," Choomka said. *"It remains unfamiliar because it is uncommon, but it has become a modern structure worth examining."*

> **Waqf is another structure for financial services professionals to understand**

HARIVANSH JEEHA, Senior Legal Adviser, Financial Crime Commission

"Are you able to detect red flags based on what the manual has told you?"

Harivansh Jeeha, Senior Legal Adviser at the Financial Crime Commission, called for better-supported reporting and closer cooperation with banks and management companies. At the 8th Financial Crime Conference, he warned that institutions need to demonstrate that their safeguards work in practice—and that failures uncovered during an investigation can bring their own conduct under scrutiny.

Financial institutions need to provide investigators with clearer, better-supported information if the country is to detect financial crime early and recover its proceeds, according to Harivansh Jeeha, Senior Legal Adviser at the Financial Crime Commission (FCC).

"What we want is well-reasoned reports on the things that genuinely matter," he told the opening day of the 8th Financial Crime Conference, making the case for closer cooperation between the commission, banks and management companies.

Speaking on September 2 at the Hilton Mauritius Resort and Spa, he linked the quality of compliance work inside institutions to the ability of investigators to follow money, establish control over corporate structures and pursue assets.

Harivansh Jeeha's session addressed the need for a proactive approach between financial institutions, management companies and law enforcement. His starting point was the shared interest in protecting Mauritius's standing as an international financial centre.

"Mauritius has built its reputation as a serious, well-regulated international financial centre and reputation is a shared asset," he said. *"It benefits banks, it benefits management companies, it benefits the country as a whole."*

That shared interest comes with different responsibilities. Investigators have powers that financial institutions do not possess. Banks and management companies, however, have access to customer relationships, transactions and corporate information that law enforcement does not have at the outset.

The effectiveness of the partnership depends on bringing those perspectives together before funds move further through the financial system.

He stressed the urgency of that work. Money can cross borders within seconds, while delays in providing useful information make tracing and recovering assets more difficult. His concern extended to the quality, completeness and timeliness of reporting: a vague account of unusual activity offers investigators a weaker starting point.

He described banks and management companies as *"two sides of the same coin"*. Management companies provide the corporate picture: the history of an entity, its ownership chain, directors, beneficiaries and the people giving instructions. Banks provide the financial picture through accounts, payments, counterparties and transaction patterns.

> **Someone can be the ultimate beneficiary of an asset without ever appearing as the director or shareholder.**

The distinction matters when the activity visible in a bank account does not correspond to the purpose described in corporate records. The senior legal adviser gave the example of a purported holding company making rapid, high-value transfers to unrelated third parties. Bringing the corporate information together with the movement of money can reveal a different picture from either source considered alone.

The examples he presented, he emphasised, came from investigations. *"They are not theoretical or textbook red flags. These are things which we have seen."* One concerned corruption proceeds moving through intermediaries or companies before being converted into investments or other assets. For banks, the warning signs included incoming funds inconsistent with the customer's profile, money moving rapidly onwards and payments involving third parties with no clear commercial connection.

Asset purchases or spending that does not fit the known financial circumstances of the customer were another concern. For management companies, the questions arise in the structure itself: whether its complexity serves a commercial purpose, why ownership or control has changed, and whether instructions are coming from someone absent from the formal records.

That last point ran through his discussion of concealed control. Corporate documents may identify shareholders and directors without revealing who directs the relationship. *"Registered ownership is not the same as effective control,"* he said. *"Someone can be the ultimate beneficiary of an asset without ever appearing as the director or shareholder."*

Harivansh Jeeha acknowledged that complex structures can have legitimate commercial purposes. The task is to understand their rationale and how they operate, including how ownership and control have evolved over time.

An initial snapshot is insufficient where the people involved subsequently change. Frequent changes in ownership or directorship, unexplained nominee arrangements and the same individuals appearing across apparently unrelated entities warrant closer examination. Material changes in ownership or control information should prompt a reassessment of risk, he argued.

Loans, investments and circular transactions formed another set of examples. A loan agreement can provide a plausible documentary explanation for money changing hands while leaving its purpose unresolved.

He highlighted repeated lending between related parties with weak repayment capacity, repayment almost immediately after disbursement and funds circulating back to their starting point. *"Is there a rationale behind it?"* he asked.

The assessment, he suggested, should bring together the parties, their ownership and control,

CONT'D ON PAGE 27

What we want is well-reasoned reports on the things that genuinely matter

the relevant approvals, the transaction pattern and the supporting documents. The existence of an agreement does not settle the question of economic substance.

His banking examples also included accounts with little activity over several years that suddenly receive substantial sums. Such a change requires examination against the customer's profile and an explanation of the source of the money.

Cross-border activity adds questions about geography, particularly where funds arrive from unexpected jurisdictions. Multiple linked accounts, connections between apparently separate entities and instructions inconsistent with a business's stated purpose can also help build the picture.

The Senior Legal Adviser's emphasis was on assessing indicators collectively and grounding concerns in specific facts. An unusual feature needs context; the combination of several features may justify further action.

"A single large payment might be nothing, but the same payment repeated with the same characteristics across months might be everything," he said. That approach has implications for the organisation of compliance work. Monitoring should detect patterns, and unusual activity needs to reach the appropriate compliance function for assessment. Recording an alert and closing it without meaningful examination does little to resolve the underlying concern.

He also raised the problem of insufficiently documented suspicious transaction reports, explaining that weak supporting information can delay investigations. He favoured thoughtful analysis over reports filed mechanically to protect an institution's position.

"Step one is to identify precisely what is unusual. You must be specific and not vague," he said when outlining a seven-step assessment process. Another step was to *"obtain and assess supporting information, ask questions, request documents"*.

His wider approach involved examining connections and corroborating evidence, referring matters for appropriate internal analysis, applying reporting obligations and preserving the records and reasoning behind the eventual decision. The rationale matters whether the institution reports the concern or decides against doing so.

Cooperation continues when investigators request information. Harivansh Jeeha called for clear contact points, timely coordination and preservation of relevant records against alteration, destruction or loss, subject to applicable requirements.

Institutions should also explain what they supply. Internal terminology, account codes and relationships may be familiar to the business but obscure to an outside investigator. *"It is good that you are able to explain to us the context in which the document is made,"* he said.

His remarks carried a warning for institutions that regard their involvement in an investigation as limited to providing evidence about a customer. Their own conduct can become relevant if investigators identify procedural failures.

"Initially, someone, a bank or an agency, or whoever, can be treated as a witness," he said. *"But should the investigation reveal that proper proceedings have not been taken by your institution, then the investigation widens."*

The practical question is whether safeguards operate as intended. Laws, policies and compliance manuals establish a framework, but investigators also examine how institutions apply them. *"Are you able to detect red flags based on what that manual has told you?"* he asked.

That question connected his operational recommendations to the broader objective of asset recovery. Corporate records, financial information and investigative evidence need to form a coherent account that can support further action.

"So, my message to you is that better information leads to better intelligence, which in turn leads to better investigations, and which in turn leads to better asset recovery."

RUBINA HOSSEN ALLY, Managing Director at Kaydan Ltd

“Beyond a box-ticking culture towards a more genuinely risk-based approach”

Rubina Hossen Ally brings more than 23 years of experience in offshore finance, fiduciary services, wealth structures and AML/CFT compliance. In this interview at the 8th Financial Crime Conference at Hilton Resort & Spa on September 2 and 3, she examines the vulnerabilities facing management companies and fiduciaries in Mauritius as well as the challenges of identifying ultimate beneficial owners, the shift from box-ticking to a genuinely risk-based culture, and the growing role and risks of technology and artificial intelligence. She also argues that the next challenge for Mauritius is to demonstrate that AML/CFT controls work effectively in practice, not merely on paper.

CONT’D ON PAGE 29

Given your 23+ years of experience in offshore finance, fiduciary services, wealth structures and AML/CFT compliance, what are the biggest vulnerabilities that management companies and fiduciaries in Mauritius need to address today, noting that the fiduciary sector is often at the frontline of financial crime risks?

Management companies are often at the frontline of financial crime risks because they are approached to establish and administer both relatively straightforward and highly complex structures, including trusts, foundations, corporate entities and special purpose vehicles.

The key vulnerability is not necessarily the complexity of the structure itself, but whether the service provider genuinely understands why the structure has been established, who ultimately controls or benefits from it, and how the assets and transactions within it are being funded.

From my perspective, management companies and fiduciaries need to focus on four fundamental areas.

First is understanding and documenting the rationale for the structure and ensuring that it is commercially and legally justified. Second, they need to understand the transactions being undertaken and assess whether they are legitimate, commercially reasonable and consistent with the client's stated activities and profile.

Third is identifying and verifying the ultimate beneficial owner, particularly where ownership and control are spread across multiple jurisdictions or vehicles.

Fourth is establishing and verifying the source of wealth and source of funds, rather than relying solely on documentary evidence without understanding the underlying circumstances.

With increasingly sophisticated ownership structures involving multiple jurisdictions, trusts and private wealth vehicles, how difficult is it to establish the true beneficial owner and source of wealth of a client?

The complexity of modern ownership structures can certainly make it more challenging to establish the true beneficial owner and source of wealth, particularly where multiple jurisdictions, trusts, foundations or private wealth vehicles are involved. However, the right questions must be asked from the outset.

It is not simply a matter of collecting KYC documents and checking that the file is complete. It is about understanding the client's objectives, the rationale behind the structure, the flow of funds and the relationship between the various entities and individuals involved.

With the right expertise, a sound understanding of AML/CFT requirements, a clearly defined risk appetite, and a good knowledge of international structuring, it is possible to look through complex structures and identify the ultimate beneficial owners and establish the legitimacy of the source of wealth.

Technology and effective screening tools also play an important role, but they should support rather than replace professional judgement. Ultimately, it is the combination of appropriate due diligence, experienced analysis and continuous monitoring that allows a service provider to have a meaningful understanding of the client and the risks associated with the structure.

Mauritius has strengthened its AML/CFT framework considerably since its FATF grey-listing experience. From an industry perspective, have we moved from a compliance-driven culture to a genuinely risk-based approach?

There has been a clear shift from a predominantly compliance-driven, box-ticking culture towards a more genuinely risk-based approach. The FATF experience was an important catalyst in this regard, as it highlighted that having policies and procedures on paper is not, in itself, sufficient.

Today, compliance is increasingly viewed as an ongoing process rather than a one-off exercise. Organisations are expected to continuously assess and understand their clients, identify emerging risks, monitor transactions and activities, and adapt their controls accordingly.

We are also seeing greater investment in technology to automate and strengthen certain compliance processes, particularly in areas such as ongoing monitoring, screening, customer risk assessments and regulatory reporting. This allows organisations to focus their resources on higher-risk areas rather than applying the same level of scrutiny across the board.

That said, I would not suggest that the journey is complete. One of the key lessons from Mauritius' experience is that a robust AML/CFT framework is not simply about having comprehensive policies and procedures in place; it is about ensuring that those policies are understood, implemented and consistently adhered to across the organisation.

So, from an industry perspective, I would say that Mauritius has made significant progress towards a genuinely risk-based culture, but the real measure of success is whether that approach is embedded in day-to-day decision-making and organisational culture, rather than simply demonstrated for regulatory compliance purposes.

Technology, artificial intelligence and digital onboarding are transforming client due diligence. Do you see technology as primarily an opportunity to strengthen AML controls, or could it also create new vulnerabilities for fiduciary businesses?

Technology and artificial intelligence can significantly strengthen AML controls by making the due diligence process faster, more consistent and more efficient. Digital onboarding, automated screening and ongoing monitoring can help management companies identify risks more quickly and allow compliance teams to focus their resources on higher-risk clients and transactions.

However, technology should remain a tool to support compliance, rather than a substitute for human judgement. There must still be appropriate human intervention to assess the information obtained, challenge anomalies and ensure that the organisation's policies and procedures are actually being followed. A system can flag a risk, but it is ultimately the compliance professional who needs to understand the context and determine what that risk means.

There is also a new dimension to consider: the security and integrity of digital data. As more sensitive client information is collected, stored and processed electronically, fiduciary businesses must ensure that their systems are robust, secure and protected against unauthorised access, cyberattacks and data breaches.

Therefore, I see technology as a significant opportunity, but one that comes with additional responsibilities. The most effective approach is to combine technology with strong cybersecurity, data governance, robust internal controls, regular system testing and, importantly, experienced human oversight.

Ultimately, the objective should not be to make AML processes entirely automated, but to use technology intelligently to make them more effective, risk-sensitive and sustainable, while retaining professional judgement at the critical decision-making points.

How should fiduciary firms strike the right balance between delivering a seamless service to legitimate international investors and applying increasingly demanding KYC, enhanced due diligence and sanctions-screening requirements?

I think the balance comes down to communication, education and the way the onboarding process is managed.

There are essentially two types of international investors. Some are already well versed in AML/CFT requirements and understand why KYC, enhanced due diligence and sanctions screening are necessary. For others, particularly those who may be less familiar with the regulatory requirements in Mauritius, it is important to explain these requirements clearly before the onboarding process begins.

The key is not to compromise on the level of due diligence, but rather to make the process clear, structured and client-friendly. It is all about the tone and approach adopted by the fiduciary firm. If the client understands from the outset what information is required, why it is required and how the process will work, what can otherwise be perceived as a tedious exercise becomes much more manageable.

Ultimately, good client service and strong compliance should not be viewed as conflicting objectives. A well-organised fiduciary firm should be able to maintain robust KYC, EDD and sanctions-screening standards while still providing a seamless and professional experience for legitimate investors.

The objective is to make the compliance process feel simple for the client, without ever making the underlying compliance requirements less rigorous.

Looking ahead to Mauritius' next round of international scrutiny, what is the one area where the financial services industry must raise its game if the country wants to demonstrate that its AML/CFT framework works effectively in practice—not just on paper?

Looking ahead, I believe the key area where the financial services industry needs to raise its game is moving from having a compliance framework to demonstrating that compliance is genuinely embedded throughout the organisation.

It is not simply a matter of appointing an MLRO and DMLRO and having a comprehensive set of AML/CFT policies and procedures in place. Those are essential foundations, but they do not, by themselves, demonstrate that the framework is effective in practice.

Compliance should not remain the sole responsibility of the MLRO or the compliance department. It is a collective responsibility across the organisation, from the board and senior management through to client-facing teams and administrators. Everyone needs to understand their role in identifying, escalating and managing financial crime risks.

The key, therefore, is good governance supported by a strong compliance culture. Senior management and the board must set the right tone from the top, but that tone must translate into the day-to-day behaviour and decision-making of the entire organisation.

Ultimately, the next level for Mauritius is to demonstrate not just that we have the right policies and controls on paper, but that those controls are understood, implemented, challenged and consistently applied in practice. That is what will demonstrate the effectiveness and maturity of our AML/CFT framework to international assessors.

SALEEM ABDULLATIFF, Barrister at Law - Associate Director, Governance, Risk & Compliance

"Boards can delegate compliance; they cannot delegate accountability!"

For Saleem Abdullatiff, financial crime is no longer a matter that Boards can leave to compliance departments. He argues that effective AML/CFT/CPF (Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing) governance must be measured by behaviour and outcomes rather than policies, training records and dashboards. From Board accountability and the limits of blind reliance on the Compliance function to the risks posed by Artificial Intelligence, deepfakes, cryptocurrencies and cyber-enabled fraud, he calls for directors to challenge information rather than simply receive it.

Has financial crime risk become a boardroom issue rather than simply a compliance issue?

It always was one. The Board of a financial institution has ultimate responsibility for the effective management of the institution, including oversight of financial crime risks.

As the governing body, the Board is expected to understand, assess and monitor the risks to which the company is exposed, and ensure that those risks are appropriately managed through an effective governance, risk management and compliance framework.

The Board may delegate certain activities to the Compliance function, which acts as the second line of defence. However, that delegation is limited to operationalising and executing the Board's high-level strategy through appropriate policies and processes. Overall responsibility for compliance, risk oversight and governance remains with the Board.

The real test is effectiveness, not paperwork. A firm may have policies, procedures and training in place and still fail if its governance and culture do not translate those measures into day-to-day behaviour. That makes AML effectiveness a boardroom issue, not merely a compliance-function issue.

What should directors personally understand about their institution's exposure to financial crime?

Directors need to understand that the framework they see is the visible output of a culture they set.

I use a simple chain: governance shapes culture, culture shapes behaviour, and behaviour produces outcomes. Regulators can inspect the last link; the Board can influence the first.

Directors therefore need to understand where the institution's real exposure sits — which clients, structures and jurisdictions carry the greatest risk; where judgement is being exercised every day by people far removed from the boardroom; and what those people believe will happen if they raise concerns about a profitable relationship.

That is where governance becomes real. It is not simply about having a framework on paper, but understanding how that framework operates in practice.

Can a board rely too heavily on its MLRO (Money Laundering Reporting Officer) and Compliance department?

Yes. I strongly believe this is one of the most common failure patterns.

Passive oversight looks like this: the Board receives reports without probing them, focuses on training completion, treats *"no issues"* as evidence of low risk, and leaves judgement entirely to Compliance.

Active oversight is different. It asks Compliance what it is actually worried about, challenges trends, exceptions and backlogs, tests whether staff feel safe escalating concerns, and links the institution's stated risk appetite to real business decisions.

The distinction I would offer is this: good governance is not simply receiving information; it is challenging information. Delegating the function is proper; delegating accountability is not. You can delegate Compliance. You cannot delegate accountability.

At the same time, there has to be a balance. Too much reliance on Compliance can result in passive oversight, while no reliance at all suggests that the control framework itself is not trusted. The objective is to establish the right balance between management responsibility and Board oversight.

What warning signs should immediately attract a board's attention?

The most underrated warning sign is silence.

I sometimes open my sessions with what appears to be a reassuring quarterly dashboard: training completed, policies updated, no overdue reviews, no internal suspicious transaction reports and no breaches. Yet six months later, regulators may identify significant deficiencies within that same firm.

Every one of those metrics measures activity. None necessarily measures behaviour.

Nothing reported, nothing escalated and nothing challenged is not necessarily assurance. It can be the loudest indicator that a culture has stopped asking questions.
Beyond that, Boards should pay attention to escalations that arrive late or only after issues have been resolved, backlogs in periodic reviews, exceptions granted to the largest relationships, and any pattern of legitimate concerns being reframed as commercial obstacles.

There is a useful test for any director: when was the last time you saw something in a Board report that made you uncomfortable?

If the answer is "never", that itself may be the finding.

When compliance failures occur, how far should directors themselves be held accountable?

The regulatory trend is clear, and Mauritius has already demonstrated it.

In The MCB Ltd v ICAC case, the fine was upheld on appeal for failing to take reasonable measures to prevent the misuse of banking services. The Court found compliance and internal audit ineffective in practice, and actual laundering did not have to be established for the regulatory breach to arise.

More recently, the FSC's 2026 enforcement actions involving Special Activity Licences, including a management company, highlighted governance failures such as funds being held for prolonged periods without escalation, inadequate due diligence at onboarding and on an ongoing basis, and the absence of an appropriate business risk assessment.

Accountability should follow the decision, not simply the job title.

Where a Board sets the tone, establishes the risk appetite and determines the resourcing — or fails to do so — it owns the consequences. Where individuals deliberately conceal information from the Board, that is a different matter.

The more important question for directors is not, "Did we approve a policy?" Rather, it is: "Would our controls survive a test of effectiveness rather than documentation?"

Are boards receiving the right information to understand emerging digital financial crime risks?

Not always. Many Boards receive regular compliance and risk reports. However, emerging digital financial crime risks — including cyber-enabled fraud, cryptocurrency misuse, artificial intelligence, deepfakes and broader digital-asset threats are evolving faster than traditional reporting frameworks.

Boards may therefore require more targeted intelligence, specialised training and forward-looking risk information if they are to effectively challenge management and fulfil their oversight responsibilities.

The challenge is to ensure that Board reporting does not simply describe what has already happened. It must increasingly help directors understand what could happen next, where the vulnerabilities are, and whether the institution is prepared to respond.