relycomply

How critical AML intelligence makes South Africa's enforcement agenda actionable.

Following the government's 2026 Budget Speech, we address an elephant in the room: the need for a cohesive, data-led AML strategy to effectively combat financial crime.

Executive summary.

South Africa's Budget Speech arrives at a time when fundamental shifts are taking place in compliance. Since being removed from the Financial Action Task Force's (FATF) grey list, following increased prosecutions and data-backed law enforcement, the government's renewed focus on preventing organised crime and illicit trade is certainly welcome. And clearly, the momentum is being maintained.

Enoch Godongwana's speech highlights the nation's plans to invest heavily in enforcement, including increased security spending, judicial obligations, and enhanced border management resources. Placing monetary value behind expertise and numbers to bolster defences is a very visible signal to crime networks. However, this is insufficient without the same investment granted to industry-wide AML capabilities to improve the shared use of necessary financial intelligence.

Organised crime syndicates threaten to adapt their digital capabilities at a rate far quicker than they can be stopped. They're no longer territorial units, but whole financial ecosystems operating online, nationwide and internationally. Being able to intercept and disrupt the laundered proceeds of contraband trading, trafficking and terrorist financing relies on financial institutions with the critical compliance infrastructure to analyse data, continually, and with sustainable risk-based programmes to adapt to the ways criminals curb even enhanced clampdowns on national security.

Enforcement cannot work alone. It relies on a collaborative financial industry unit that must spot suspicious transactional activity on the frontlines, and how their bolstered partnerships with RegTech providers, regulators, and the South African government can provide sufficient evidence that makes intended criminal capture and prosecution possible.

This report explores how AML compliance – from identifying risk signals to increasing intelligence sharing – can provide the foundational backbone to dismantle criminal networks using the very systems they wish to exploit, facilitating the country's strong enforcement response needed in today's digitalised financial crime frontier.

The scale of South Africa's enforcement response.

When South Africa found itself on the FATF greylist in February 2023 for insufficient AML/counter terrorist financing (CFT) governance, there were plenty of shortcomings to rectify. A historically poor state capture record, a lack of international cooperation, and low prosecutions were key areas to address out of a 22-item Action Plan drawn up in conjunction with FATF.

The road to delisting required ample cooperative effort to work through this set of reforms and to take strengthened AML from the abstract to the actual, comprising a partnership among the government, regulators, the South African Revenue Service, and law enforcement agencies. Following the introduction of a specialised digital intelligence unit, enforced sanctions, and increased beneficial ownership transparency, the Plenary deemed the Action Plan items completed, and South Africa was taken off the greylist in October 2025.

Continual commitment is required to pass FATF's ongoing Mutual Evaluation, but a brighter path has been paved for the way the nation is tackling criminal enterprise, namely, reforms to rectify FATF's 11 Immediate Outcomes such as demonstrating a national CFT risk assessment strategy, increased investigation and prosecution rates, and the implementation of data from the Financial Intelligence Centre (FIC) to support law enforcement efforts.

So much so that the FATF delisting was well noted in the 2026 Budget Speech as a major turning point in South Africa's approach to tackling organised crime; Minister of Finance Enoch Godongwana announced that "the world has taken notice" of South Africa's credibility and commitment to "tangible results".

Now, the government is doubling down on a strategy to bolster territorial integrity against organised crime, using **R848.2 billion** over the medium term, including:

- R291.2 billion to be spent on peace and security by 2028/9, an increase from R268.2 billion, to "intensify law and order".
- R1 billion is being allocated to the South African Police Service (SAPS), and an additional R1 billion to the South African National Defence Force (SANDF) through the Criminal Assets Recovery Account (CARA) – which have been deployed conjunctively to tackle illegal mining, gangsterism, and organised crime.
- The Border Management Authority received an added R990 million to fill 738 positions to better manage immigration laws and the seizure of illicit goods flowing into the country.

Sector	Budget allocation	Purpose
Peace & security	R291.2B	Intensify law and order
SAPS + SANDF	R2B	Joint operations against illegal mining, gangsterism, and organised crime
Border management authority	R990M	Fill 738 positions, manage borders & seizures

It has been noted by the National Budget Treasury review that such fiscal allocations aim to strengthen ethical, safe and developmental communities in South Africa. This is all well and good in that organised crime has long proven a systemic and economically crippling practice, with the state accounting for that fact. However, added funding to services is not an answer to the problem, and the work is not over to enact world-class national security.

As evidenced in the steps toward delisting, increased enforcement is far from a numbers game and instead a tactical, collaborative approach that takes the financial system into consideration. On the frontline of handling cross-border payments, accountable institutions are the backbone for identifying suspicious behaviours and conducting AML that actionably leads to the prevention of organised crime.

Brushing up on criminal typologies and regulatory best practices is only the start. It takes a wealth of financial intelligence – as well as platforms that can process, track and alert anomalous data – to actually take the fight against savvy criminal networks and realise the enforcement agenda that has been thoughtfully planned up to this point.

Organised crime as its own financial ecosystem.

It is reductive to believe that organised crime networks are only territorial units. Given the interconnectedness of the digital world, corruption in one country may be funded by offshore financiers, and illicit supply chains can continue via savvy trade-based money laundering (TBML) techniques.

This only concerns 'on the ground' crime too; the digital economy opens the floodgates for the use of hard-to-trace crypto payments and crypto-mixers, and even dark web marketplaces to compile and sell stolen identities that ensure complex criminal structures remain opaque. Real victims can be pulled into the underworld via investment or romance scams to conduct illegal fund flows on behalf of a fraudster.

The opportunities open to criminals – acting evermore like enterprise-level businesses in their global operational fluidity and digital capabilities – are limitless. What ties them together are AML vulnerabilities in the financial industry, where ongoing gaps make the entire sector a systemic enabler for crime to continue evading capture by law enforcement.

South Africa is well-positioned to rise to the challenge. Yet while it excels in some areas, some critical criminal pockets still thrive. Measures for combatting organised crime are outlined in the Prevention of Organised Crime Act (POCA), while the country is recognised by TRACIT as one of Africa's most industrialised economies, albeit one with pervading illegal commerce involving alcohol, tobacco, pharmaceuticals, wildlife trafficking, and mining (as the Budget Speech prioritised).

Supply chain networks also suffer within cross-border shipping routes, online marketplaces and the country's free trade zones (FTZs), while the informal economy is made up of 7.5 million people, growing at a rate to outpace the formal economy.

AML compliance is paramount to discovering and nullifying these activities by criminal syndicates, due to the simple fact that their proceeds of crime must be flushed through the system somehow. Traditionally, placement, layering and integration are methods utilised, which rely on the following:

- **Multiple bank accounts:** by smurfing proceeds, launderers can transfer small donations below risky thresholds into accounts, then continually shift them via the same branches and institutions, or to international accounts to make the initial deposit tough to trace.

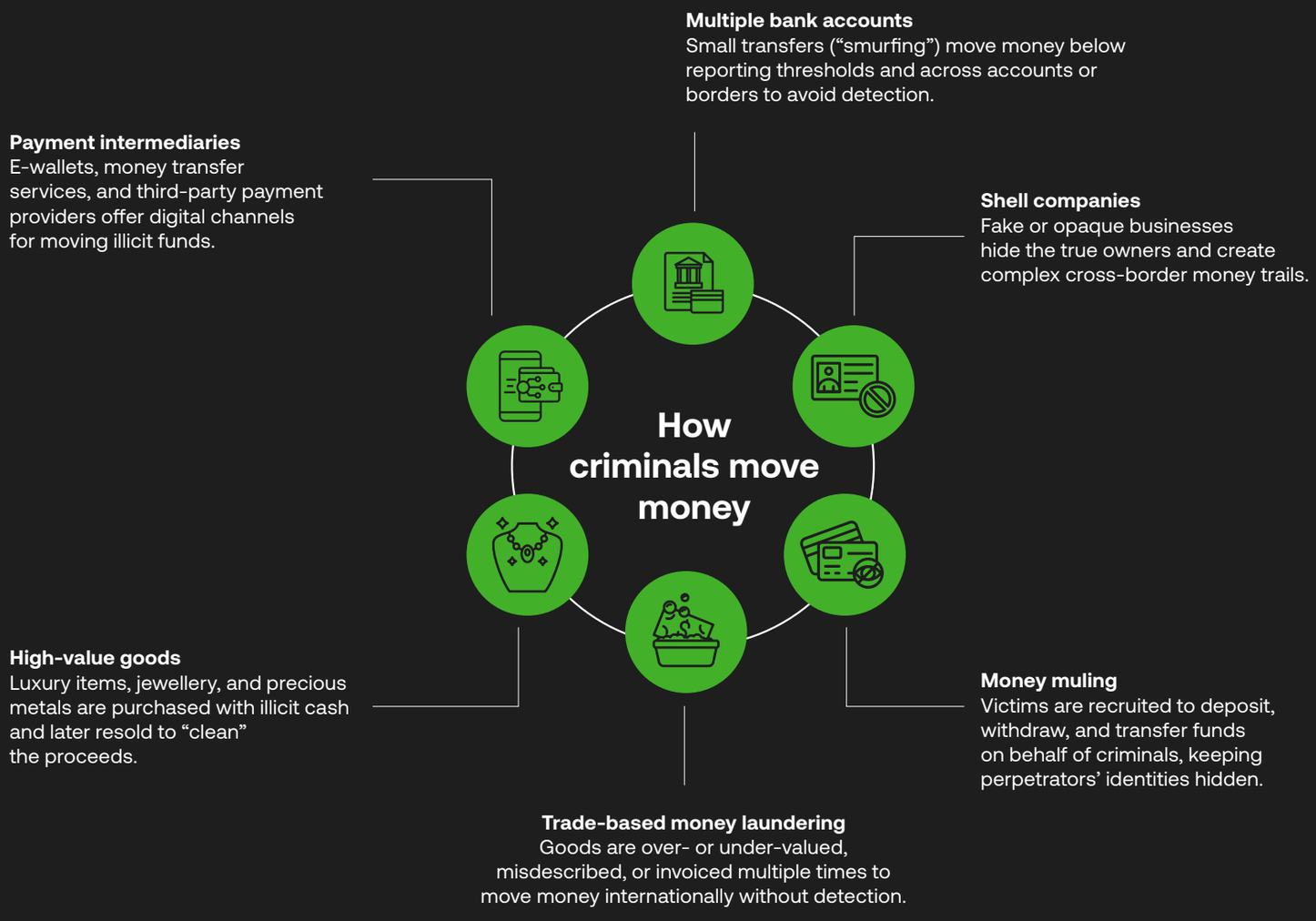
- **Shell companies:** some accounts may be registered with fake businesses that appear to be legitimate, usually set up in jurisdictions with lax compliance and tax rules, to cover for beneficial owners and create an obfuscated cross-border money trail.

- **Money muling:** victims can be recruited to deposit, withdraw and move illicit funds around the system on a criminal organisation's behalf, separating perpetrators from the money.

- **TBML:** criminals may over- or under-value exported goods, falsely describe their items, or invoice multiple times to shift money overseas, bypassing the formal system.

- **High-value goods:** huge sums of illicit cash can be used to purchase luxury lifestyle items, jewellery, and precious metals to be resold elsewhere, thus 'cleaning' the proceeds of crime.

- **Payment intermediaries:** e-wallets, money transfer services and third-party payment providers offer new payment rails for criminals to exploit digitally.



With the rise of digital finance and South Africa's high digital adoption rates, laundering is being reinvented to accommodate biometric identity fraud and cryptocurrencies to evade capture. These pose additional risks to older populations or less digitally native areas of the population, where confidence around these quickly changing technological innovations will be lacking, and they will look to who they bank with to protect them. Therefore, financial institutions must understand criminals' new routes and typologies to not only recognise the very real risks they pose, but also to disrupt the flow of money. If you freeze activity and seize the proceeds, you can terminate operations. This essentially deprives criminals of the funds they use to commit further schemes and halts the instruments they use to do so.

Even further, financial institutions that share their intelligence as part of a wider inter-agency investigative effort can help discover complex organisation structures and dismantle them from the top down; beneficial ownership transparency is a growing topic within anti-financial crime regulation that could effectively discover hard-to-find owners responsible for overseeing networks.

In positive news, TRACIT also notes that R7.5 billion was allocated in April 2025 to bolster SARS's enforcement of illicit trade, improving the seizure of illicit gold, mispriced customer items, and crypto-related items. However, the sustainability of this practice relies on more resources than the Minister of Finance has recently proposed, and also a greater focus on strengthening public-private intelligence loops.

After all, accountable financial companies are key figures in South Africa's increased prosecution goal. True disruption begins with continuous monitoring of data at the transaction layer to detect behavioural risk in suspicious accounts, ensuring they're not mere conduits for organised crime.

relycomply

R7.5 billion

boosted enforcement - but long-term impact needs more funding and stronger public-private intelligence.

The data challenge of international trade beyond border security.

An interconnected globe will always grant avenues for criminals to hide. Regional trade laws, voluminous e-commerce activity and digital payments are ensuring that illicit movements will only get more sophisticated, unless compliance wakes up to the extent of the problem.

In April 2023, South Africa introduced the Border Management Authority (BMA). With the intention of seizing counterfeit goods and enforcing immigration laws, the governmental body has faced its own internal problems of understaffing and budgets; namely, a shortfall of over R4 billion, with over 8,000 vacancies in 2025. Not to mention recent news surrounding corruption amongst BMA officials.

However, South Africa's Budget Speech has ramped up momentum to enhance cross-border security, part of a concerted effort over time to intercept illegal goods and proceeds of crime that is so integral to stopping international networks. This includes filling 738 new border positions and allocating R990 million to the BMA.

The problem is that this physical presence and fiscal backing can't provide complete cross-border security. Digital capabilities will also need to be up-to-scratch with global standards (and the skills of laundering professionals), as cross-border payment infrastructure threatens to crumble in the face of evolving payment rails and currently unregulated cryptocurrencies.

Understanding mispricing and false invoicing common to trade-based money laundering (TBML), which is when criminals move money through trade transactions to disguise its origin, relies on detecting unusual patterns or anomalies in large volumes of financial data across different formats. This is something that financial institutions (FIs) must be able to facilitate to connect effectively with port and border authorities. Sharing relevant financial and transaction data is the next enabler to raise cross-jurisdictional risk awareness in earnest, alongside better visibility of who ultimately owns and benefits from companies (beneficial ownership). This enables institutions to be far more proactive in preventing organised crime.

There is, luckily, good news for South Africa's digital payment innovation. SARB has already been a major proponent for SWIFT ISO2002 payments; the leading standard for structured payment data, granting FIs the ability to contextualise the nature of transactions for high-risk transaction behaviours. Likewise, SARB's work with the National Treasury has seen the creation of the National Payments Utility (PEM) and PayInc, a platform to support real-time payment and settlement interoperability between a broad range of PSPs, including banks, fintechs and non-financial entities.

SA's roadmap to airtight compliance

ISO 20022:
Leading the shift to structured payment data for high-risk detection.

PEM & PayInc:
Real-time settlement interoperability between banks and fintechs.

The Travel Rule:
CASPs must now share originator/beneficiary data for crypto.

Capital Framework:
Assets now governed within cross-border movement frameworks.

While crypto assets are not currently recognised as legal tender, crypto asset service providers (CASPs) are accountable institutions under the FIC Act to register and report suspicious activity to the FIC. Elsewhere, 2025's Travel Rule requires CASPs to share originator and beneficiary data for any crypto-related payments in line with FATF standards – and the Budget outlined these assets to be "governed in the cross-border movement of capital framework".

There is certainly an intent to clamp down on cross-border payment mistreatment. Evolving a widespread payments infrastructure is dependent on understanding global and local AML frameworks, storing and sharing transparent financial data, and collaborating instantly with financial intelligence centres, besides simply bolstering personnel in the BMA.

Underlying anti-fincrime technology is the beating heart for gaining real-time visibility of any high-risk cross-border activity, and must be a standard across South Africa's ecosystem for actual enforcement to be airtight.

relycomply

Enhancing conviction: the Budget Speech's focus on the judicial system.

The endgame of all AML compliance investigations is the judicial process, guided by evidence supplied that can eventually result in prison time for heinous organised crime. With leading perpetrators behind bars and their funds frozen, FIs, police forces and governments can start to cut the heads from the Hydra, diminishing the effect of proliferating activity while subsequent criminals scramble to fill the gaps, on the backfoot.

In light of this and South Africa's troubling state capture records, growing judicial capacity announced in the Budget Speech is a welcome addition, as follows:

- An allocated sum of R687 million has been reserved for increased use in the judicial systems.
- Around R888.8 million will be shifted from the Department of Justice and Constitutional Development to the Office of the Chief Justice, to manage budgets independently––with similar arrangements planned to fund Parliament.
- Specialised courts have been announced, with allocations considered later this year pending cost finalisations.
- Commissions of inquiry already underway, but not expected to finish by their deadlines, will also receive funding.

Strengthening judicial capacity

R687 million	allocated to judicial system strengthening.
R888.8 million	shifted to the Office of the Chief Justice for independent budget management.
Specialised courts	announced, with funding to be finalised.
Commissions of inquiry	extended funding for ongoing investigations.

On the surface, this will grant an extended amount of power to increase convictions. However, court time and case resolution are only as strong as the evidential data used. Policing and judicial capacity does not operate in a vacuum, and specialised courts are only able to act efficiently when well-governed institutions enable proper reporting protocols. In financial crime situations, this relies on tying individuals to fund flows and tracing ultimate beneficial owners to wrongdoing within convoluted organisational structures. As highlighted at the Financial Sector Conduct Authority (FSCA) Conference, regulatory effectiveness increasingly depends not only on enforcement capacity but on the quality, explainability, and auditability of underlying financial data used to evidence misconduct.

Of course, this is not easy when syndicates continue to mask their behaviour through sophisticated techniques. Financial institutions will simply be unable to back up criminal reporting without structured, accurate and quality intelligence as required by the FIC. A network of banks, courts, and regulators needs to be just as well coordinated, as so often, gangsterism can continue when financial data is fragmented between systems. That's especially true if SARs are manually handled and contain human error. FSCA discussions reinforced that fragmented data environments and inconsistent governance frameworks create supervisory blind spots, particularly where AI and automated decisioning systems are involved without sufficient oversight.

Enforcement is only as strong as the data behind it. Fragmented data doesn't just slow investigations - it lets crime slip through.

The shift to standardisation: Twin Peaks and COFI.

A positive change to address such fragmentation is South Africa's unifying Twin Peaks model. On one hand, it has seen the introduction of the FSCA, supervising proper market conduct and the fair treatment and education of financial customers. The integrated model also established the Prudential Authority (PA) to oversee the safety and soundness of accountable institutions under the Financial Services Regulation (FSR) Act. The Twin Peaks model is particularly significant for financial crime prevention, as it strengthens coordination between conduct oversight and systemic risk supervision — both critical when identifying patterns of illicit financial flows that may otherwise remain siloed across institutions.

Further, the next phase of the reform will look to harmonise existing financial sector rules into a solidified framework for market conduct regulation in the upcoming Conduct of Financial Institutions (COFI) Bill. FSCA's positioning of COFI signals a shift away from checklist compliance toward outcome-based accountability, requiring firms to demonstrate that governance frameworks, controls, and decisioning processes lead to fair and transparent outcomes in practice. Driven by stricter governance and customer-oriented responsibility, a single regulatory model embeds proactive financial crime prevention as a baseline necessity. Importantly, COFI elevates accountability to the board level, reinforcing that responsibility for financial crime risk management, data integrity, and customer outcomes cannot be delegated to systems alone.

Essentially, the COFI Bill ties together regulated institutions' detection and data audit capabilities, the FIC's extended analysis on submitted intelligence, and eventually increased convictions in courthouses as one complete ecosystem. This reflects a broader regulatory direction highlighted by the FSCA: a move toward continuous oversight supported by stronger governance, clearer auditability, and improved visibility across institutional data environments.

To achieve this and bridge the extensive gap between initial criminal action and final prosecution, greater adoption of regulatory technology (RegTech), meaning technology that helps institutions meet compliance and financial crime requirements more efficiently, is needed across South Africa's regulated ecosystem. Especially in such high-scrutiny environments as banking, fintech, payments, insurance and asset management, this type of compliance technology provides an ongoing, credible defence system to facilitate end-to-end compliance that keeps up with fundamental shifts in the regulatory market, including proper adherence to upcoming requirements under the COFI Bill. As regulatory expectations evolve, institutions will increasingly need to evidence how decisions are made, how risk is assessed, and how financial crime controls operate in practice, not simply that they exist on paper.

Why RegTech is the essential defense system

Reduces human error
Automated workflows minimise repetitive mistakes in SAR reporting and compliance processing.

Strengthens identity verification and auditability
Verify identities and trace suspicious transactions with real-time accuracy.

Enables connected intelligence ecosystems
Better data governance leads to shared intelligence and faster investigations.

Shortening the alert-to-conviction timeline requires responsible AML design and compliance maturity: automated systems that reduce SARs' repetitive human error, verify identities accurately, and trace suspicious transaction audits. When digital advancement is instilled across the board, more cooperative investigation efforts can run with shared financial intelligence. They're integral to hindering organised crime more quickly than it takes criminals to invent new ways to exploit holes between institutions. In this context, Twin Peaks supervision and COFI's principles-based framework together create a stronger foundation for connected compliance ecosystems, where better data governance leads to stronger intelligence, faster investigations, and ultimately more effective prosecution outcomes.

pKYC: from periodic checks to holistic vigilance.

Despite being ‘organised’, crime simply doesn’t operate on a timetable. It is adaptive, networked, and opportunistic by design. This was always the case before the digital boom, and it is even more so now that it operates across every level of in-plain-sight and underground channels. When networks can keep dirty money flowing through the system, they can recruit new worker bees and support various criminal ventures anywhere in the world, every minute of the day.

The Budget Speech’s efforts to stop these proceeds of crime must not end at paying for more human resources at the borders, but must create a clear shift toward automated, continuous monitoring of every fund movement from every entity. It must also reflect a structural shift toward real-time financial intelligence embedded within the financial system itself. Because, on the FIs’ compliance side, reviews of high-risk customers and companies might happen annually at best. And even less for those deemed less risky, as little as every five years. This creates a fundamental timing mismatch between criminal activity and compliance detection.

Closing the window of opportunity for criminals

The criminal reality

Networks are adaptive, interconnected, and operate 24/7. They don’t follow a calendar.

The compliance gap

Traditional reviews happen every 1–5 years. This creates a “timing mismatch” where illicit funds flow freely between check-ins.

The pKYC solution

Moving from calendar cycles to behavioral activity. If the risk changes at 2:00 AM, the profile should update at 2:00 AM.

You can’t stop a real-time threat with a five-year plan.

There's simply no way to be as dynamic as highly organised groups if this carries on. Customer risk profiles must evolve in line with behavioural activity, not calendar cycles. Know your customer (KYC) protocols that were once static must have a consistent second-by-second eye on goings-on, including payment behavioural changes such as rapid deposits and withdrawals of minuscule or hefty sums.

However, the concept of "Perpetual KYC" (pKYC) is often misunderstood. While frequently associated with repeated screening or periodic resubmission of documentation, many institutions still treat it as an enhanced version of batch-based compliance rather than a continuous intelligence model. True pKYC is not periodic automation - it is continuous, event-driven risk monitoring. Traditional approaches such as scheduled ID refreshes or periodic sanctions rescreening remain fundamentally manual and insufficiently responsive to evolving financial crime typologies, including cyber-enabled fraud, illicit trade networks, and cross-border laundering operations.

Nor is pKYC some sort of silver bullet to solve all problems. It represents a structural shift in compliance architecture, not a standalone solution. Shifting decades of static rules-based compliance processes at every accountable institution is massive, especially toward such powerful risk intelligence. After all, effective pKYC has to monitor a range of interconnected parties: politically exposed persons (PEPs) watchlists, beneficial ownership changes, and aforementioned typologies that make the proceeds of crime harder to find. Screening and monitoring must therefore move toward dynamic, continuously recalibrated risk scoring models that adjust in real time based on customer behaviour and network relationships.

At the same time, pKYC cannot operate effectively without governance and human oversight. Like all advanced automation systems, it requires explainability, auditability, and human validation to ensure that alerts are accurate, proportionate, and actionable. Without this, continuous monitoring risks generating excessive false positives, overwhelming compliance teams and reducing investigative effectiveness — directly undermining the objective of improved risk detection.

The challenge, therefore, is not whether pKYC is needed — that is already clear — but how it is implemented. Poorly executed perpetual monitoring can introduce operational friction, customer disruption, and system inefficiencies that increase costs without improving outcomes. Treating pKYC as a simple "switch-on" upgrade is a misconception. Instead, it requires modular deployment, phased integration, and alignment with existing risk frameworks.

This is where RegTech partnerships become essential. Modern RegTech solutions enable institutions to assess pKYC readiness, integrate real-time monitoring capabilities, and calibrate risk engines according to sector-specific exposure, geographic footprint, and customer complexity. Rather than functioning as a compliance add-on, pKYC becomes part of a broader financial crime prevention architecture.

The Budget may highlight the growing scale and sophistication of illicit trade and organised crime. However, a meaningful response requires shifting financial institutions from periodic compliance gatekeepers to continuous intelligence nodes within the financial crime ecosystem. When implemented correctly, pKYC becomes not just a compliance upgrade but a foundational layer in strengthening national and institutional resilience against
financial crime.

Making public-private intelligence actionable.

This raises a prevailing AML question in South Africa and globally: how can real-time financial sector integration truly work at scale? With multiple jurisdictions involved and significant budget allocations directed toward enforcement, border control, and institutional strengthening, the absence of fully standardised, interoperable financial intelligence frameworks remains a core barrier to effectively disrupting organised crime networks.

In theory, the system should operate in two complementary layers: through the "visible investments" outlined in the 2026 Budget Speech, and the "invisible infrastructure" enabled by pKYC, shared intelligence frameworks, and structured SAR reporting.

The former works to make a clearer enforcement effort a shared enterprise between SARS, the Border Management Authority, and the deployment of SANDF alongside the police force–a combination of human presence and guiding regulatory principles. Additionally, the Budget Speech highlights opportunities for greater private-sector participation to streamline procedural requirements, close regulatory gaps, and clarify institutional roles. Elsewhere, the finance minister said that amendments to Public Private Partnerships (PPP) regulations should be a public institution's go-to for enforcement cases, whereby limitations in capacity or capital also reduce the effectiveness of implementation.

Visible vs. invisible defense

The visible investment	SAPS, SANDF, and Border Management Authority (BMA)	Public-Private Partnerships (PPPs) to close capacity gaps	Human presence and regulatory principles
The invisible infrastructure	pKYC and shared intelligence frameworks	Structured, real-time SAR reporting	Interoperable systems like PayInc

Of course, organisations that work in tandem can only improve the compliance culture, especially following joint efforts leading to South Africa's delisting. However, it is financial institutions that function as the primary data conduits for public-private intelligence sharing, processing high-volume, high-velocity transactional data that often contains the earliest indicators of financial crime activity.

Effective cooperation between government, regulators, and the private sector—including banks, fintechs, and accountable institutions—requires a shared commitment to disrupting the proceeds of crime. Critical financial intelligence should not remain siloed across institutions, but instead be shared through secure, governed mechanisms that allow for timely intervention and coordinated enforcement.

Secure intelligence sharing mechanisms

The success of initiatives such as PayInc's shared digital payments infrastructure (previously PEM) demonstrates how interoperable systems can support secure, high-volume financial transactions across institutions. On the regulatory side, the South African Anti-Money Laundering Integrated Task Force (SAMLIT), established by the FIC, reflects a growing shift toward structured public-private intelligence collaboration, bringing together:

- The SARB's Prudential Authority and Financial Surveillance Department
- The South African Banking Risk Information Centre (SABRIC)
- The Banking Association South Africa (BASA)
- 22 national and international banks

Already, SAMLIT's coordination between financial institutions and regulators has showcased how financial intelligence can be used to disrupt complex illicit markets, including the illegal wildlife trade. This provides a scalable blueprint for expanding similar collaborative models across other forms of trade-based and financial crime.

Faster feedback loops and response

With financial institutions supplying SAPS and other enforcement bodies with structured, real-time intelligence—aligned with their obligations to the FIC—there is an opportunity to create a closed-loop enforcement ecosystem where detection, analysis, and prosecution are more tightly integrated.

To achieve this effectively, institutions require a proactive shift toward pKYC and continuous transaction monitoring frameworks that generate contextual, real-time risk intelligence rather than periodic reports. This enables the production of higher-quality Suspicious Activity Reports (SARs), which can be more easily operationalised into investigations, arrests, and prosecutions. Standardised reporting formats and unified data models are essential to reducing response latency across agencies.

RegTech as the 'collaborative glue'

The ability to process, analyse, and act on large-scale financial data in real time is increasingly dependent on RegTech infrastructure. These solutions act as an operational layer between financial institutions and regulatory expectations, enabling scalable compliance, automated monitoring, and cross-border alignment with evolving AML obligations.

Rather than functioning as standalone tools, RegTech platforms increasingly serve as the integrating layer that connects KYC, transaction monitoring, sanctions screening, and reporting into a unified compliance ecosystem.

With appropriate governance and deployment, these systems enable both public and private sector actors to respond at the speed required to match modern organised crime networks. AI-enabled RegTech also allows institutions to adapt to shifting typologies, jurisdictional differences, and evolving regulatory expectations across multiple markets.

Ultimately, while the Budget Speech outlines the foundations of a more collaborative enforcement environment, it also points to a broader reality: financial crime is already globally interconnected, and financial intelligence systems must be equally interconnected to remain effective.

Financial data's foundational role In enforcement.

The intention behind the Budget Speech's increased security allocation is a welcome and visible signal of intent. Illicit trade and money laundering activity—whether facilitated through physical borders, digital channels, or cross-border financial systems—continues to pose a systemic threat to national economies, including South Africa, particularly as it strengthens its AML posture following FATF scrutiny and mutual evaluation pressures.

While the government acknowledges the scale of the problem, the next enforcement frontier lies in transforming anti-financial crime spending into measurable outcomes and long-term return on investment. This requires shifting from enforcement-as-spend to enforcement-as-intelligence infrastructure. In practical terms, this means shared financial intelligence must be capable of identifying not just suspicious activity, but the underlying networks, beneficial ownership structures, and systemic enablers that allow illicit capital to move undetected.

This is especially critical given the increasing risk of capital flight, where poorly traced or irregularly documented transactions enable funds to exit jurisdictions undetected, undermining tax bases and weakening macroeconomic stability.

Organised financial crime, therefore, functions not only as a law enforcement issue, but as a structural economic risk. Its prevention must be embedded within national economic policy, regulatory design, and financial infrastructure strategy. In this context, AML should no longer be viewed as a compliance obligation or operational burden, but as a core component of fiscal resilience and national security.

Every transaction tells a story.

The question is whether we're reading it in time.

Connected financial data is the new frontline of enforcement.

Conclusion.

Banks, fintechs, and payment service providers should not be positioned merely as regulated entities operating under constraint, but as critical infrastructure within the financial system that actively supports economic stability through transaction visibility, risk detection, and real-time monitoring capabilities enabled by pKYC and advanced compliance systems.

With improved data sharing and stronger AML frameworks enabled through RegTech partnerships, both national and cross-border enforcement efforts can be significantly strengthened. This creates a more coordinated ecosystem where public and private sector actors operate as interconnected intelligence nodes, capable of responding to financial crime in real time rather than retrospectively.

In a global financial system defined by interconnectivity, enforcement capability must be equally networked. This requires a level of institutional alignment that mirrors the sophistication and coordination of organised crime networks themselves.

Ultimately, we cannot arrest our way out of a globally networked financial crime ecosystem. For meaningful disruption to occur, South Africa must continue to build a compliant, data-driven financial infrastructure that is capable of supporting real-time intelligence sharing and coordinated enforcement. By leveraging RegTech and modern AML systems, the narrative must shift from viewing compliance as a cost centre to recognising it as a strategic national security and economic stability asset.


relycomply®
AML and KYC. Unified. Automated. Scalable.