



FINANCIAL FLOWS AND KEY INDICATORS ASSOCIATED WITH ILLICIT FINANCIAL FLOWS AND TRADE-BASED MONEY LAUNDERING IN SOUTH AFRICA

PERIOD | MAY 2026

IFFs AND TBML EXPERT WORKING GROUP

SAMLIT MEMBERS

Public sector

Financial Intelligence Centre
South African Reserve Bank: Financial Surveillance department and Prudential Authority.

Industry bodies

South African Banking Risk Information Centre
The Banking Association South Africa

Banks operating in South Africa

Absa Group Limited
African Bank Limited
Albaraka Bank
Bank of China
Bank of Taiwan South Africa Branch
Bidvest Bank Limited
Capitec Bank Limited
China Construction Bank Corporation, JHB Branch
Citibank N.A., South Africa
Deutsche Bank AG, JHB Branch
Discovery Limited
Finbond Mutual Bank
FirstRand Bank (RMB and FNB)
GBS Mutual Bank
Grindrod Bank Limited
Grobank Limited
HBZ Bank Limited
Habib Overseas Bank Limited
HSBC Bank
Investec Bank Limited
JP Morgan Chase
Nedbank Group Limited
Sasfin Bank Limited
Standard Chartered Bank
State Bank of India, South Africa
Standard Bank of South Africa Limited
TymeBank Limited

ACKNOWLEDGEMENT

This report is a product of collaboration across the SAMLIT IFF and TBML expert working group (EWG). The EWG acknowledges the contributions of all participating financial institutions for supplying risk return responses, typology inputs, cross-border risk data, and practical control insights used in the anonymised analysis.

The EWG acknowledges the technical input from the Financial Intelligence Centre (FIC), the South African Reserve Bank (SARB), the Prudential Authority (PA), and the South African Revenue Service (SARS - Customs and Excise).

International standard setters whose guidance informed this report include the FATF, the Egmont Group, UNCTAD, UNODC, Global Financial Integrity, and the Wolfsberg Group.



DISCLAIMER

The information in this publication is for information purposes and for raising awareness on illicit financial flows and trade-based money laundering in South Africa and has not been independently verified. This report does not constitute legal, regulatory, supervisory, or enforcement advice. All institutional information is aggregated and anonymised and no institution is named. Views expressed are those of the SAMLIT EWG and do not necessarily reflect official positions of any participating institution or public authority.

CONTENTS

1. Executive Summary	7
2. Introduction	9
2.1 Background	9
2.2 Purpose of the report.....	9
2.3 Scope	10
2.3 Limitation	10
2.4 Methodology.....	10
3. Global and regional context	11
3.1 Global trends.....	11
3.2 Regional African trends	12
3.3 Implications for South Africa	12
4. South Africa's Exposure: External evidence.....	12
4.1 Trade and macro-economic context.....	12
4.2 External estimates of illicit flows via trade	13
4.3 Commodities and trading partners of concern	13
4.4 Institutional and supervisory assessments.....	14
4.5 Measuring and monitoring IFF	15
4.6 Key takeaways from external evidence	15
5. Supervisory insights from bank risk returns.....	15
5.1 Scope, grouping and confidentiality	15
5.2 Identification of channel misuse and control posture	16
5.2.1. Why cards and EFTs matter for cross-border IFF.....	16
5.3 Products and services identified as vulnerable	16
5.4 What a correspondent banking chain is, and where opacity arises	17
5.5 High-risk jurisdictions identified by banks	18
5.6 Anonymised supervisory vignettes (illustrative).....	18

5.7 Supervisory observations and implications	19
6. Triangulation: External vs supervisory evidence.....	19
6.1 What the two lenses show	19
6.2 Corridors and commodities: points of convergence	19
6.3 Channels and typologies: how value moves	20
6.4 Correspondent chains: transparency and route behaviour	20
6.5 Where the evidence converges most strongly	20
6.6 What the triangulation implies for supervisory focus.....	21
6.7 Towards an analytics blueprint that connects payments to goods.....	21
7. FIC Regulatory Reporting Data	21
8. Consolidated typologies, red flag indicators, and case studies.....	22
9. Joint public-private actions and implementation pathways.....	27
9.1 Purpose and framing	27
9.2 Cards and EFTs: reducing cross-border leakage on high-velocity rails.....	27
9.3 Trade-payment integrity: aligning payments with goods and services.....	28
9.4 Correspondent chains: keeping originator/beneficiary data intact and routes explainable	28
9.5 Information-sharing, feedback loops, and case uplift.....	29
9.6 SARS information requirements and TBML payment-trade linkage	29
9.7 Joint public-private implementation pathways	35
10. Conclusion	37
11. Recommendations.....	38
Annexures	40

Abbreviations:

Term	Definition
AML, CFT and CFP	Anti-money laundering, combating the financing of terrorism and combating the financing of proliferation
ATMS	Automated transaction monitoring systems
BOP Code	Balance of payments code – SARB classification for cross-border transactions
CASP	Crypto asset service provider
CBDDQ	Correspondent banking due diligence questionnaire (Wolfsberg Group)
CDD, EDD	Customer due diligence, enhanced due diligence
CIB	Corporate and investment banking
CIPC	Companies and Intellectual Property Commission
CNP	Card not present transaction
CTR	Cash threshold report (filed with FIC for cash above R49 999.99)
DMCC	Dubai Multi Commodities Centre
DRC	Democratic Republic of the Congo
EFT	Electronic funds transfer
EWG	Expert Working Group
FATF	Financial Action Task Force
FCY	Foreign currency
FI	Financial institution
FIC	Financial Intelligence Centre (South Africa)
FICA	Financial Intelligence Centre, 2001 (Act 38 of 2001)
FinSurv	Financial Surveillance Department (SARB)
FSCA	Financial Sector Conduct Authority
FTZ	Free trade zone
FX / Forex	Foreign Exchange
GFI	Global Financial Integrity
HS Code	Harmonised system code – international product classification
IFF	Illicit financial flows
IFTR	International funds transfer report
ISO 20022	Financial messaging standard for payments data
IWT	Illegal wildlife trade
KYC	Know your customer
MCC	Merchant category code

MER	Mutual evaluation report (FATF)
ML	Money laundering
MSB	Money services business
MVTS	Money or value transfer services
PA	Prudential Authority (SARB)
PTA	Payable-through account
RBB	Retail and business banking
RMA	Relationship management application
SADPMR	South African Diamond and Precious Metals Regulator
SAMLIT	South African Anti-Money Laundering Integrated Task Force
SAR	Suspicious activity report
SARB	South African Reserve Bank
SARS	South African Revenue Service
SBLC	Standby letter of credit
SCF	Structured commodity finance
SDA	Single discretionary allowance (R1 million per calendar year)
STF	Structured trade finance
STR	Suspicious and unusual transaction report
TBML	Trade-based money laundering
TF	Terrorist financing
TPR	Terrorist property report
UNCTAD	United Nations Conference on Trade and Development
UNODC	United Nations Office on Drugs and Crime
Wolfsberg	Wolfsberg Group (association of global banks developing financial crime risk frameworks)

1. Executive Summary

South Africa's exposure to illicit financial flows (IFF) via trade and payments is material, cross-border, and multi-channel. External evidenceⁱ highlights commodity-centric risks - especially gold - and persistent partner country discrepancies characteristic of trade mis-invoicing. Supervisory insights, aggregated from anonymised bank returns, show how value moves through the regulated sector on high-velocity retail rails, via cards and EFTs, and along trade payment practices such as advance payments and document light transactions. Triangulated together, these lenses point to a consistent picture of South Africa's IFF and TBML exposure – concentrated in commodity corridors (notably gold), retail payment rails (cards and EFTs), and multi-hop correspondent chains – and support a focused set of joint public-private actions to address IFF and TBML more effectively.

Mirror trade analyses identify significant discrepancies in South Africa's commodity trade statistics, particularly in gold that may be consistent with trade misinvoicing and warrants further investigation.

These patterns align with global (TBML typologies: over or under-invoicing, multiple invoicing, phantom shipments, and harmonised system (HS) code abuse, often facilitated by weak documentation and opaque intermediaries. At the same time, bank-reported data indicate three recurring payment vectors: Cash-in followed by foreign cash-out on cards; card-to-crypto or retail-foreign exchange ("FX/Forex") spend; and EFT pass-throughs or third-party payments (including via non-resident foreign currency accounts). Across correspondent banking chains, risk concentrates where originator and beneficiary data degrade across multi-hop routes, or nested relationships obscure the true parties.

This assessment is presented in the context of South Africa's removal from the FATF list of Jurisdictions under Increased Monitoring on 24 October 2025, and is intended to support the sustainability commitments given by South Africa to the FATF.

Corridors and commodities

Jurisdictions repeatedly identified by participating banks as presenting elevated IFF and/or TBML risk in respect of their customers' cross-border activity – namely the UAE, China and Hong Kong, Kenya, Uganda, Pakistan, Nigeria, Mozambique, Zimbabwe and the DRC – overlap with international reporting on commodity hubs, re-export centres, and regional trade lanes. This convergence supports corridor-focused analytics that connect payment behaviour with trade declarations (price bands, grades, International Commercial Terms ("Incoterms"ⁱⁱ)).

What South African institutions report

In anonymised group aggregates, large banks report broader detection and control coverage for card or EFT-driven cross-border risks (e.g., scheme crypto, quasi-cash rules, geo or velocity limits, single discretionary allowance (SDA) monitoring, automated detection). Small and medium banks emphasise trade payment exposure (advance payments, documentary checks). Many institutions

ⁱ "External evidence" throughout this paper refers to independent international and open-source evidence drawn from FATF, Egmont, UNCTAD, GFI and academic studies external to the South African banking sector.

ⁱⁱ the standardised International Chamber of Commerce trade delivery terms defining seller/buyer responsibilities, cost and risk transfer points, e.g. FOB, CIF, DAP.

report formal correspondent risk assessments and increasing attention to message quality (complete travel rule fields, low repairs) and route analytics (unexpected hubs, repeated intermediaries).

Joint public-private actions (12-18 months)

- **Cards and EFTs:** Align on control baselines (scheme crypto or quasi-cash rules; geo or merchant category code (MCC) filters; velocity thresholds), publish a behavioural analytics library (e.g., cash-in followed by foreign cash-out intervals; card not present (CNP) bursts to emergent forex (FX) or crypto acquirers), and enhance purpose of payment consistency for selected outward EFTs (notably advance payments and third-party beneficiaries).
- **Trade payment integrity:** Pilot payment-trade congruence testing in priority corridors; implement advance-payment triggers and documentary anchors; focus on price-volatile commodities (e.g., gold) where mirror trade anomalies and bank flags converge.
- **Correspondent chains:** Benchmark travel rule completeness and repair rates; deploy route analytics for off-route hubs and chain-length outliers; uplift visibility into nested activity using Wolfsberg constructs.
- **Information sharing and feedback:** Translate confirmed case typologies into machine-readable features; introduce structured case tags across participants for trend analysis; establish a nimble, privacy-respecting lane for emerging merchant clusters or intermediary routes.
- **Measuring progress:** Track a small, outcome-oriented indicator set (e.g., blocked or reviewed crypto or quasi-cash attempts; advance payment congruence hit rates; wire message completeness and repair trends in priority corridors).

What success looks like

Over the plan horizon, participating institutions and public agencies should see:

- (i) reduced leakage on cards and EFTs (lower incidence of cash-in followed by foreign cash-out sequences and CNP bursts to risky merchants),
- (ii) higher precision in trade payment escalations (better priceband or mirror flags and documentation outcomes), and
- (iii) cleaner correspondent data (higher travel rule completeness; lower repairs; fewer unexplained off-route hubs).

Collectively, these outcomes reflect a practical, risk-based tightening of South Africa's defences against IFF that is achievable through public-private co-operation.

2. Introduction

This research report is based on the identification of TBML as a financial crime threat to the banking system in South Africa. The report deals with IFF related to TBML. The research is intended to provide a global and South African context of IFF related to TBML to enhance understanding of this money laundering phenomenon. Ultimately, the research report is intended to improve detection techniques of these transactions and increase regulatory reporting.

2.1 Background

IFF represent a persistent challenge to global financial integrity and economic stability. These flows involve the cross-border movement of money or value that is illegally earned, transferred, or utilised¹. TBML is one of the most complex and adaptive forms of IFF, it disguises the movement of illicit value through legitimate trade transactions².

Globally, IFF are estimated to amount to hundreds of billions of US dollars annually³, undermining revenue collection, distorting trade statistics, eroding the tax base, and facilitating organised crime, corruption, and terrorist financing. For South Africa, as a trade-dependent emerging economy and regional financial hub, exposure to TBML and broader IFF risks is particularly significant⁴.

2.2 Purpose of the report

This report has been developed by the SAMLIT IFF and TBML Expert Working Group to provide a clear, evidence-based understanding of South Africa's exposure to IFF and TBML risks, and to support a co-ordinated public-private response aligned with national and international AML/CFT priorities.

The report aims to:

- Provide a structured overview of global and regional trends in IFF and TBML, drawing on authoritative international sources (including FATF, UNCTAD, OECD, GFI, and the Egmont Group).
- Analyse South Africa's exposure to IFF and TBML risks by integrating external research with domestic supervisory and industry data.
- Identify key risk drivers, including high-risk products, services, transactional behaviours, jurisdictions, and corridors linked to IFF.
- Compare international typologies with domestic supervisory insights to identify areas of convergence, divergence, and potential blind spots.
- Translate typologies and risk indicators into actionable insights to strengthen detection, monitoring, and escalation capabilities across financial institutions.
- Develop targeted policy, supervisory, and operational recommendations to enhance South Africa's anti-money laundering and combating of terrorist financing (AML and CFT) framework, consistent with FATF standards and regulatory mandates.
- Support strengthened collaboration between the banking sector, regulators, law enforcement, and SAMLIT stakeholders in mitigating IFF and TBML risks.

2.3 Scope

The scope of this report encompasses a consolidated and triangulated analysis of multiple data sources and intelligence streams to provide a comprehensive view of IFF and TBML risks in South Africa. Specifically, the report:

- Aggregates anonymised industry findings from participating financial institutions, including identified IFF and TBML typologies, high-risk corridors, transactional red flags, and control effectiveness across products and services.
- Incorporates Financial Intelligence Centre (FIC) data, including TBML-linked suspicious transaction and activity reports for the period 2022/23 to 2024/25.
- Draws on Prudential Authority supervisory data, including risk-return submissions from 25 local banks, to highlight products, services, and jurisdictions most associated with IFF vulnerabilities.
- Integrates open-source and international research to contextualise domestic findings within global and regional IFF and TBML trends.
- Aligns analysis with South Africa's FATF 2021 mutual evaluation findings and post-grey list reform priorities, particularly in relation to improving understanding and disruption of complex cross-border laundering typologies.

All findings presented in this report are based on aggregated and anonymised inputs. No individual institution is identified, ensuring confidentiality while enabling system-wide insights and strengthening collective risk understanding.

2.3 Limitation

The report does not attempt to provide a precise monetary estimate of IFF in South Africa beyond what is already available in open-source studies. Instead, it contextualises available estimates with qualitative supervisory insights to build a comprehensive risk picture. The analysis relied on publicly available international research, supervisory information, industry submissions and regulatory reporting data. No academic institutions or external organisations were consulted.

2.4 Methodology

The analysis was based on two complementary sources of evidence:

1. Open-source reports and research
 - FATF and Egmont Group reports on TBML typologies and risk indicators⁵.
 - UNCTAD, OECD, and Global Financial Integrity (GFI) studies on trade misinvoicing and IFF measurement³⁴.
 - Regional research on Africa's exposure to IFF and capital flight⁵.
2. Prudential Authority risk returns (25 Banks)

- Standardised responses to questionnaires submitted by local banks.
- Key questions relating to identification of IFF or TBML risks, controls implemented, and high-risk jurisdictions.
- Thematic coding and aggregation of responses to identify common patterns, divergences, and supervisory insights.

By combining international evidence with domestic supervisory data, the report aims to provide a balanced and practical assessment that can inform supervisory planning, inter-agency co-operation, and engagement with foreign counterparts. Jurisdictional findings were derived from frequency analysis of aggregated bank submissions and were not weighted by transaction value, customer volume or exposure size.

3. Global and regional context

IFF and TBML present a significant global and regional challenge that provides essential context for understanding South Africa's exposure. At the global level, evidence points to material fiscal losses from trade misinvoicing, commodity-centric vulnerabilities (particularly gold, diamonds, and oil), and the systematic exploitation of financial and logistical gateways such as free trade zones and multi-hop correspondent banking chains. At the regional African level, the continent is disproportionately affected relative to the size of its economy, with commodity corridors (notably gold routed via Dubai), re-export hubs (Nairobi, Dar es Salaam, Johannesburg, Mauritius and Hong Kong), and structural weaknesses in data integration, analytical capacity, cross-border informality and governance compounding vulnerability.

These global and regional trends translate directly into elevated risk for South Africa given its commodity export profile, regional financial hub status, and trade corridor alignment with several high-risk jurisdictions. A detailed exposition of global trends, regional African trends and their implications for South Africa – including the underlying statistics, typology cases, commodity vulnerability data, geographic hub mapping and structural challenge assessment (with accompanying charts) – is set out in Annexure A.

3.1 Global trends

Global evidence consistently demonstrates that IFF undermine financial system stability, with UNCTAD estimating annual losses of USD 88-150 billion for developing countries due to trade misinvoicing and GFI finding that in some economies IFF may account for as much as 20 per cent of all trade flows. Against the backdrop of a global trade system exceeding USD 32 trillion annually, TBML techniques – over- and under-invoicing, multiple invoicing, misclassification under incorrect tariff codes, and phantom shipments – are used to disguise the movement of illicit value, with precious metals (gold, diamonds), electronics, textiles, automobiles and heavy machinery among the most exploited commodities. These techniques are facilitated by falsified documentation, complicit intermediaries, the proliferation of free trade zones (now numbering more than 5 400 worldwide), and opacity in correspondent banking chains. Full detail, including illustrative FATF/Egmont case

studies from Latin America, Asia and the Middle East and the accompanying IFF and TBML chart, is set out in Annexure A.

3.2 Regional African trends

Africa is disproportionately affected by IFF, with the AU/ECA High-Level Panel (Mbeki Report, 2015) estimating annual losses exceeding USD 50 billion and subsequent studies (UNCTAD 2020, GFI 2021, Ndikumana & Boyce 2021) confirming that the order of magnitude remains materially unchanged – including USD 588 billion in cumulative trade misinvoicing across 30 African countries between 1970 and 2018, equivalent to nearly a third of total capital flight from the continent. Commodity-driven vulnerabilities dominate the regional picture: gold (under-invoiced at origin and routed via Dubai for refining and re-export), oil (Nigeria and Angola), diamonds (West Africa) and cocoa/timber (West and Central Africa) have each been systematically mispriced or misrouted to disguise value transfers. Key geographic hubs (Dubai, Nairobi, Dar es Salaam, Johannesburg, Mauritius and Hong Kong) concentrate TBML activity, while structural challenges – including data integration gaps between customs authorities and FIUs, weak analytical capacity for mirror trade and price-band checks, high informality in cross-border trade, and governance/corruption risks – compound the continent's exposure. The full analysis, illustrative country cases (Tanzania, Nigeria, West Africa), commodity vulnerability scoring, geographic hub mapping and structural challenge diagnostics (with accompanying charts) are set out in Annexure A.

3.3 Implications for South Africa

South Africa's commodity export profile – particularly gold and other precious metals – its status as southern Africa's commercial and financial hub, and its trade corridor alignment with several high-risk jurisdictions (notably Dubai, Hong Kong, Mozambique and Kenya) mean that the global and regional TBML trends outlined above translate directly into domestic exposure rather than remaining a distant or external phenomenon. Structural weaknesses observed elsewhere on the continent – limited integration between customs and financial intelligence, weak application of mirror trade analytics, and cross-border enforcement gaps – also resonate with South Africa's current supervisory and enforcement environment, reinforcing why exposure must be understood through both a global and a regional lens and providing the foundation for the external evidence assessed in Section 4 and the supervisory evidence analysed in Section 5. The full commentary, including detail on commodity exposure, trade corridor alignment, regional financial hub risk, and supervisory/enforcement gaps (with the accompanying "Implications for South Africa" chart), is set out in Annexure A

4. South Africa's Exposure: External evidence

4.1 Trade and macro-economic context

South Africa is a trade-dependent economy, with goods and services exports consistently contributing around one third of gross domestic product (GDP) and imports averaging just over 30 per cent of GDP¹⁶. This high degree of openness underscores both the opportunities and vulnerabilities associated with international trade. SARS trade statistics confirm that the country maintains persistent but fluctuating trade surpluses. For example, in December 2024, SARS reported

a surplus of R15.5 billion, reflecting the scale and velocity of cross-border flows processed through Customs¹⁷. The South African Reserve Bank's quarterly bulletin further highlights the importance of goods trade, noting that net gold exports remain a structural component of the current account balance¹⁸. A high trade-to-GDP ratio means that even small percentages of mispriced or misreported trade can translate into material IFF. When combined with South Africa's role as a financial and logistics hub for the region, this creates heightened exposure to TBML.

4.2 External estimates of illicit flows via trade

Quantitative estimates from international organisations point to significant TBML-related risks for South Africa. Global Financial Integrity's (GFI) 2018 country study – drawing on bilateral merchandise trade data from UN Comtrade, SARS, and World Bank tariff databases for 2010 to 2014 – estimated potential government revenue losses of approximately US\$ 7.4 billion annually, or US\$ 37 billion over the five-year period, attributable to trade misinvoicing⁴. Of this, US\$ 4.8 billion per year was linked to import misinvoicing, accounting for an estimated US\$ 2.1 billion in lost VAT and US\$ 596 million in uncollected customs duties, with a further US\$ 2.1 to 2.5 billion per year in company income tax losses attributed to the same practices. While the methodology has known limitations – including the exclusion of some partner data and informal flows – the magnitude of the losses indicates that trade misinvoicing represents a substantial fiscal risk to South Africa.

Complementing this, UNCTAD's 2016 analysis of primary commodities revealed a striking anomaly in South Africa's gold trade. Between 2000 and 2010, South African statistics recorded only US\$ 2.3 to 2.8 billion in non-monetary gold exports, whereas trading partners reported US\$ 59.7 billion in corresponding imports – a discrepancy of nearly US\$ 57 billion that cannot be explained by timing or classification differences alone and points to systemic under-invoicing¹². From 2011 onwards, South Africa reclassified all gold exports as "non-monetary," complicating direct comparability, yet partner-reported imports continued to show material discrepancies through 2014. UNCTAD concluded that such gaps are *prima facie* indicators of IFFs and recommended targeted investigation of the gold sector.

Taken together, these studies – despite covering different time frames and applying different methodologies – provide consistent evidence that South Africa faces material exposure to trade misinvoicing, with precious metals as a core vulnerability.

4.3 Commodities and trading partners of concern

External evidence highlights specific commodities and partner countries where risks are most concentrated. Gold remains the dominant area of concern. According to UNCTAD's partner-country analysis, the largest reported destinations for South African non-monetary gold exports between 2000 and 2014 were India (34.5 per cent), Hong Kong (17.3 per cent), Italy (13.3 per cent), and the United Kingdom (12.0 per cent)¹². High concentration in a limited number of trading partners is consistent with global TBML typologies, where illicit actors exploit established commodity corridors to move value covertly²³.

Beyond gold, iron ore exports have also raised concerns. UNCTAD noted episodic misinvoicing patterns in South African iron ore exports, particularly in trade with the Netherlands, China, and Japan¹². These discrepancies merit further scrutiny, especially given the scale of South Africa's mineral

exports. Both cases – gold and iron ore – highlight how TBML techniques such as over or under-invoicing, misclassification, and third-party payments can exploit commodity flows that dominate the country's export profile.

4.4 Institutional and supervisory assessments

International assessments have also pointed to systemic weaknesses in South Africa's framework for combating IFF and TBML. FATF's 2021 Mutual Evaluation Report acknowledged that the country has a solid legislative base but found significant effectiveness gaps, particularly in the areas of pursuing complex money laundering cases, ensuring transparency of beneficial ownership, and detecting cross-border illicit flowsⁱⁱⁱ. In February 2023, FATF placed South Africa under increased monitoring (the "grey list"), citing the need for stronger enforcement and inter-agency co-ordination.

Since the February 2023 grey-listing, South Africa has executed a structured programme of reform against the 22 Action Items agreed with the FATF, anchored in the *General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act, 2022*. The reform programme materially strengthened the legal architecture most relevant to the IFF and TBML risks addressed in this report: beneficial ownership transparency for legal persons and trusts through the CIPC and Masters' Offices; an expanded politically exposed person regime; strengthened targeted financial sanctions for terrorism and proliferation financing; risk-based supervision of designated non-financial businesses and professions by the FIC; and expanded regulatory oversight of crypto asset service providers and other previously under-regulated sectors. These were reinforced by a demonstrable and sustained increase in investigations and prosecutions of complex money laundering and the full range of terrorist financing activity, an updated National TF Risk Assessment, and enhanced inter-agency co-ordination through SAMLIT, the Fusion Centre and the Inter-Agency Working Group on Illicit Financial Flows, together with the piloting by SARS of a digital Traveller Management System for cross-border cash and bearer negotiable instrumentsⁱⁱⁱ.

Following an on-site assessment by the FATF Africa Joint Group in July 2025, the FATF Plenary on 24 October 2025 confirmed that South Africa had completed its Action Plan within the agreed timeframes and removed the country from the list of Jurisdictions under Increased Monitoring, alongside Burkina Faso, Mozambique and Nigeria. National Treasury, the FIC and SARS have been unambiguous that delisting is a milestone and not a terminal outcome: sustainability of the reforms, continued effectiveness of enforcement, and the country's readiness for its next mutual evaluation depend on sustained public-private co-operation of the kind advanced through this EWG. For the purposes of this report, the reform programme narrows – but does not close – the structural exposures identified in Sections 3 to 6: commodity-corridor mis-invoicing, high-velocity retail payment leakage, correspondent-chain opacity, and CASP-mediated cross-border value transfer remain live risks that fall squarely within the sustainability commitments given to the FATF and are the operational focus of the joint actions proposed in Section 9^{iv}.

ⁱⁱⁱ Also see [\[ifcreview.com\]](https://ifcreview.com), [\[thomsonwilks.co.za\]](https://thomsonwilks.co.za) [\[fic.gov.za\]](https://fic.gov.za), [\[sars.gov.za\]](https://sars.gov.za)

^{iv} Also see [\[fatf-gafi.org\]](https://fatf-gafi.org), [\[fatf-gafi.org\]](https://fatf-gafi.org), [\[treasury.gov.za\]](https://treasury.gov.za) [\[treasury.gov.za\]](https://treasury.gov.za), [\[fic.gov.za\]](https://fic.gov.za), [\[sars.gov.za\]](https://sars.gov.za)

4.5 Measuring and monitoring IFF

South Africa has also been included in international efforts to develop statistical measures of IFF. As co-custodians of Sustainable Development Goal Indicator 16.4.1, UNCTAD and the United Nations Office on Drugs and Crime have piloted methods for quantifying IFF. Between 2018 and 2022, South Africa participated in pilot projects testing the Partner-Country Method Plus and the Price-Filter Method Plus for detecting trade misinvoicing⁹. The pilots confirmed both the feasibility and challenges of applying these methods, highlighting the need for coordinated data collection across Customs, tax authorities, and the financial sector.

These initiatives demonstrate that South Africa has the technical capacity to adopt official IFF statistics, but they also emphasise the importance of institutionalising the process. Without sustained investment in data quality, inter-agency co-operation, and analytical capacity, measurement will remain *ad hoc* and insufficient to inform policy and enforcement.

4.6 Key takeaways from external evidence

External evidence consistently points to several conclusions:

- Scale of risk: Studies by GFI and UNCTAD confirm that South Africa faces billions of dollars in potential losses annually due to trade misinvoicing, with gold as a primary vulnerability.
- Commodity corridors: Partner-country data show persistent discrepancies in exports of gold and iron ore, with high concentration in a few destinations such as India, Hong Kong, and the Netherlands.
- Systemic weaknesses: FATF evaluations identify gaps in effectiveness, particularly in cross-border enforcement and beneficial ownership transparency, which are directly relevant to TBML detection.
- Measurement opportunities: South Africa's participation in UN-led pilots provides a credible pathway for institutionalising IFF measurement, but requires stronger integration of supervisory, Customs, and FIU data.

This evidence provides an essential external perspective that will be compared with supervisory insights in Section 5, enabling a comprehensive understanding of South Africa's exposure to TBML and IFF.

5. Supervisory insights from bank risk returns

5.1 Scope, grouping and confidentiality

This section synthesises anonymised supervisory information drawn from the Prudential Authority's risk return questionnaire (Questions 13.3.2-13.3.11). Results are presented for two cohorts: Group 1 (large banks, n = 5) and Group 2 (small and medium banks, n = 20). All statistics are shown only in aggregate at group level; no institution is named and no combination of attributes enables re-identification.⁽³⁷⁾

5.2 Identification of channel misuse and control posture

Banks report material exposure – and active mitigation – across retail payment rails. Among large banks, 60% (3/5) report that they have identified abuse of debit/credit cards and electronic fund transfers (EFTs) to facilitate cross-border IFF, and 80% (4/5) report that they have implemented controls to mitigate these risks. In the small and medium cohort, 25.0% (5/20) report identified abuse, and 50.0% (10/20) report implemented controls. Across both cohorts, institutions report a strongly enforced “no-override” posture on systems that prevent detection or reporting; this is 0/5 “Yes” (100% “No”) among large banks and 1/20 “Yes” (95% “No”) among small and medium banks, indicating that real-time rules and screening are applied at runtime. ⁽³⁷⁾

5.2.1. Why cards and EFTs matter for cross-border IFF

Debit and credit cards and EFTs are high-velocity, high-reach rails that move value across borders without the documentary discipline typical of trade finance. The return therefore asks whether banks have identified abuse of these channels and implemented controls. Three recurring patterns are reported.

First, “cash-in, card-out offshore.” Local cash deposits or opaque credits precede foreign ATM withdrawals or rapid spend at offshore merchants. The transaction looks like normal card use but economically functions as a value transfer mechanism. Large banks describe allowance-based monitoring and pattern controls for such sequences. ⁽³⁷⁾

Second, “card-to-crypto / card-to-FX platforms.” Card-not-present spend to crypto-asset exchanges or retail FX platforms can affect near instant cross-border value transfer. Where scheme or merchant identifiers exist, banks apply rule-based blocks or reviews; where merchants are new or obfuscated, they rely on behavioural or velocity analytics and merchant-category inferences. ⁽³⁷⁾

Third, “EFT pass-throughs and third-party payments.” Outward EFTs to unrelated third parties abroad – particularly via non-resident foreign-currency accounts acting as pass-throughs for non-resident-to-non-resident flows – dilute the link between payer, goods/services, and payment. FATF’s wire-transfer standard (Recommendation 16) requires complete originator/beneficiary information to accompany payments; missing or inconsistent data elevates risk. ⁽⁶⁾⁽⁷⁾⁽⁸⁾⁽³⁷⁾

Control families described by banks align with these risks: scheme-level crypto/“quasi-cash” rules, geo/velocity limits, behavioural monitoring (e.g., cash-in then rapid foreign cash-out; spikes to high-risk MCCs), purpose-of-payment validation for certain outward EFTs (especially advance payments), third-party payer/beneficiary review, and strict no-override enforcement at runtime. ⁽⁶⁾⁽⁷⁾⁽⁸⁾⁽³⁷⁾

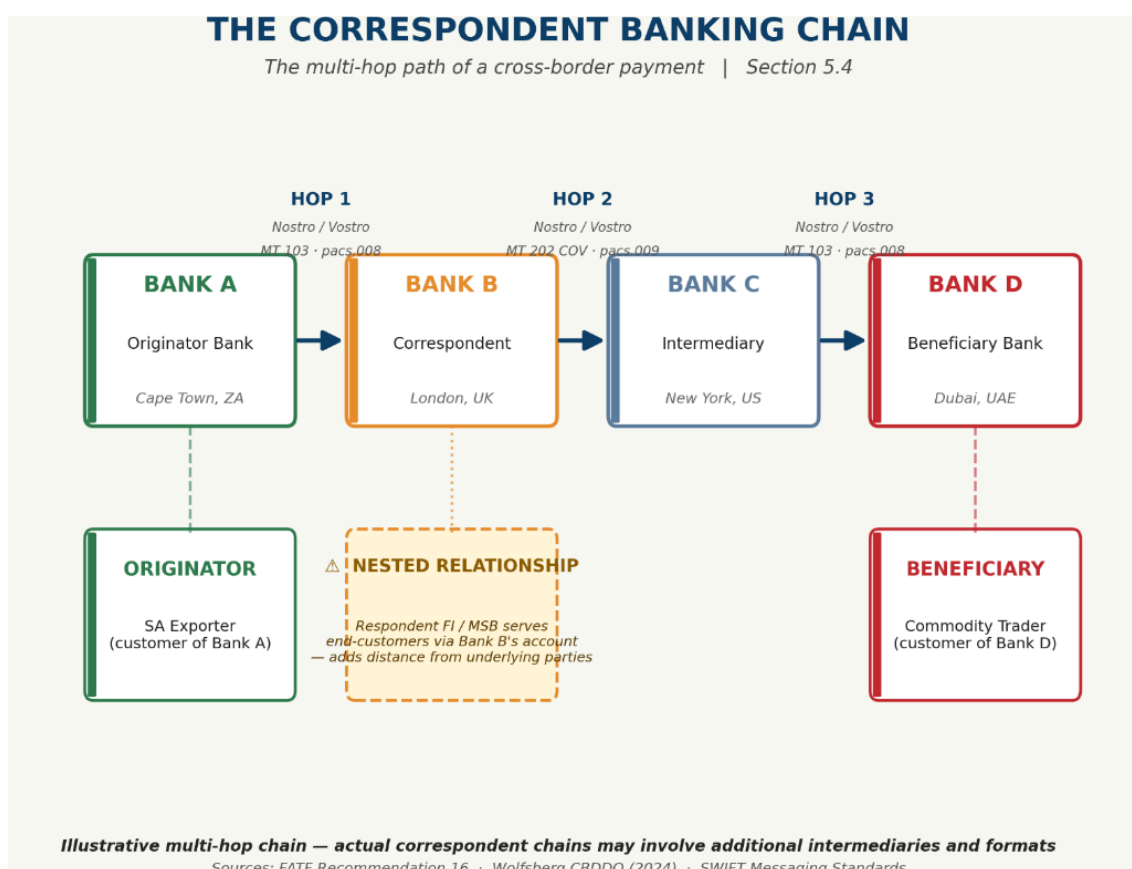
5.3 Products and services identified as vulnerable

A higher share of large banks report having identified specific products or services that could be abused, with 80% (4/5) doing so compared with 35.0% (7/20) of small and medium banks. The narrative responses point to distinct thematic profiles. Large bank portfolios describe card-funded offshore cash withdrawals, card-to-crypto/FX spend, monitoring of single discretionary allowance (SDA) utilisation, and misuse of non-resident foreign currency accounts as pass-throughs for

payments between non-resident parties with no South African footprint. Control sets referenced include sanctions pre-screening, transaction-limit and velocity rules, automated transaction-monitoring scenarios tuned for cross-border activity, and enhanced due diligence for higher-risk accounts. Small/medium banks more often foreground trade-payment exposure – notably advance payments and document-light trades – and reference targeted monitoring and documentary checks.⁽³⁷⁾

5.4 What a correspondent banking chain is, and where opacity arises

A correspondent banking chain is the multi-hop path a cross-border payment takes when the originator's bank and the beneficiary's bank do not have a direct account relationship. Bank A (originator) sends funds to Bank B (its correspondent), which may pass them to Bank C, and so on, until payment reaches the beneficiary bank. Each hop relies on nostro or vostro accounts and on message formats (legacy MT or ISO 2002 MX) to carry originator, beneficiary, and purpose fields.



In principle, FATF Recommendation 16 requires full originator and beneficiary data to travel with the payment. In practice, repairs, truncation or format mapping across hops can degrade data quality; nested relationships (where a respondent serves another FI/MSB that serves end-customers) add additional distance between the bank executing the payment and the underlying parties. Industry baselines such as the Wolfsberg Correspondent Banking Due Diligence Questionnaire frame expectations on correspondent KYC, nested-activity visibility, and payable-through restrictions. Banks in our dataset report formal correspondent-risk assessments – 80% (4/5) of large banks and 50.0% (10/20) of small/medium banks – and a focus on message quality and monitoring (including route

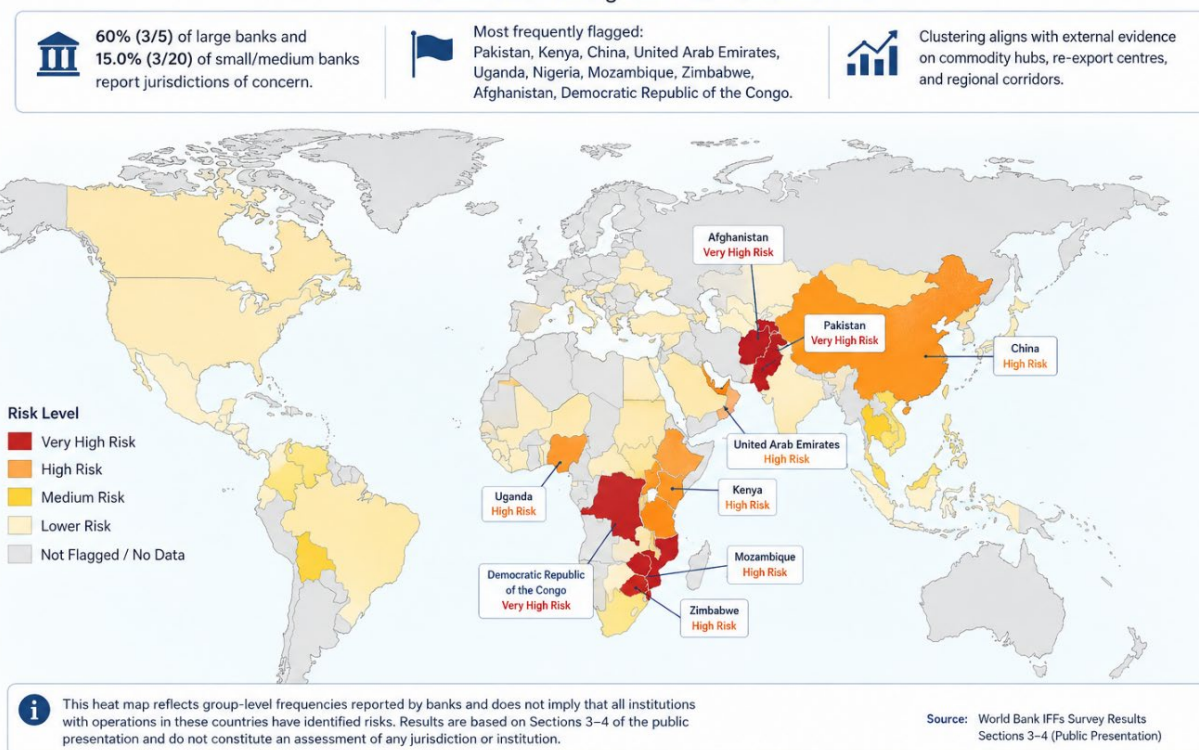
analytics, intermediary profiling, and targeted sampling of payments linked to advance-payment trades) to maintain payment transparency.^{(6) (38) (37)}

5.5 High-risk jurisdictions identified by banks

A subset of banks report maintaining jurisdictional views of customer use of high-risk countries for IFF. 60% (3/5) of large banks and 15.0% (3/20) of small and medium banks report that they have identified specific jurisdictions of concern. Aggregating across both cohorts, the jurisdictions that were most frequently referenced by participating institutions in relation to identified cross-border IFF risks are Pakistan, Kenya, China, the United Arab Emirates, Uganda, Nigeria, Mozambique, Zimbabwe, Afghanistan, and the Democratic Republic of Congo. This clustering aligns with external evidence on commodity hubs, re-export centres, and regional corridors discussed in Sections 3-4; in the public presentation, these results are shown only as group-level frequencies without associating any jurisdiction with a particular institution.⁽³⁷⁾

World Heat Map: High-Risk Jurisdictions Identified by Banks

Customer Use of High-Risk Countries for IFFs



5.6 Anonymised supervisory vignettes (illustrative)

Narratives provide concrete illustrations of risk pathways. Large-bank portfolios describe cash-in followed by foreign cash-out on cards, increased card-not-present transactions to crypto and retail FX platforms, and controls anchored in card-scheme rule sets, single discretionary allowance-limit monitoring, and rule expansion to capture emerging merchants. They also describe non-resident foreign currency accounts acting as pass-throughs for non-resident-to-non-resident payments with no local footprint, addressed through onboarding EDD and account-use scrutiny. Small and medium

banks commonly highlight advance-payment exposures and document-light trades, where validation of underlying supply-chain evidence and third-party payer/beneficiary checks are central to mitigation. These examples are paraphrased for confidentiality and illustrate patterns rather than attribute conduct to any institution.⁽³⁷⁾

5.7 Supervisory observations and implications

Three observations emerge from the group comparison. First, large banks report broader detection and control coverage for card and EFT-driven cross-border risks – consistent with more complex product suites and investment in card-scheme rules, behavioural analytics, and SDA monitoring.

Second, small and medium banks report greater emphasis on trade-payment risk (e.g., advance payments) and targeted controls; this focus complements, rather than duplicates, the emphasis on retail payments as seen in large banks.

Third, the jurisdiction clustering reported by banks aligns with the commodity and corridor patterns surfaced in Sections 3–4 – reinforcing the value of trade-payment congruence testing and third-party payer/beneficiary review in those lanes. Together, these insights provide a supervisory basis for prioritising channel-specific monitoring and corridor-focused analytics within South Africa’s risk-based approach.⁽³⁷⁾

6. Triangulation: External vs supervisory evidence

6.1 What the two lenses show

Viewed together, the external evidence and the supervisory returns tell a coherent story about South Africa’s exposure to IFF via trade and payments.

External studies emphasise commodity-centric vulnerabilities—especially gold—and highlight partner-country discrepancies and corridor concentration as recurring features of TBML.¹² GFI’s country study quantifies order-of-magnitude fiscal losses associated with trade misinvoicing, while UNCTAD’s mirror trade analysis shows substantial gaps in non-monetary gold reporting versus trading partners.^{4 12} Supervisory data surface channel-specific patterns in retail payment rails (cards and EFTs) and in trade-payment practices (e.g., advance payments, document-light trades), with larger institutions describing broader control families on card/EFT risks and smaller institutions focusing more on trade-payment exposure.³⁷

The two perspectives are complementary: one maps where value can be moved and disguised in the trade system; the other shows how funds travel through regulated payment rails and correspondent chains.^{6 7 8}

6.2 Corridors and commodities: points of convergence

External sources repeatedly associate TBML with commodity hubs and re-export centres, including destinations central to the gold trade.¹² The supervisory returns report jurisdictional clustering—notably United Arab Emirates, China, Kenya, Uganda, Pakistan, Nigeria, Mozambique, Zimbabwe and the DRC—consistent with commodity routes, regional trade corridors, and South-South payment

lanes seen in global typologies.^{37 7 8} While the lenses differ (mirror trade anomalies vs. banks' risk flags), the overlap on hubs and corridors supports targeted supervisory attention to payment-trade congruence in these lanes, particularly where gold and other high-value, price-volatile commodities are implicated.¹²

6.3 Channels and typologies: how value moves

The supervisory narratives indicate three recurring channel typologies in the card/EFT space: cash-in, card-out offshore; card-to-crypto/FX; and EFT pass-throughs/third-party payments (including the use of non-resident foreign currency accounts for non-resident to non-resident flows).³⁷ These patterns align with FATF/Egmont TBML indicators (third-party payers/beneficiaries, limited documentation, rapid value conversion) and with the wire-transfer transparency requirements in FATF Recommendation 16.^{6 7 8} In trade-payment practices, banks highlight advance payments and document-light transactions as higher-risk structures, resonating with external typologies where over/under-invoicing, misclassification, and phantom shipments are common TBML mechanisms.^{7 8} Together, the evidence suggests that documentary gaps and third-party intermediation in both payments and trade are central drivers of risk.

6.4 Correspondent chains: transparency and route behaviour

External standards (FATF) and industry baselines (Wolfsberg) stress that originator/beneficiary information must travel intact through correspondent chains and that banks should understand any nested activity in respondent networks.^{6 38} The supervisory returns confirm that banks conduct formal correspondent-risk assessments—with large banks doing so more frequently—and describe controls aimed at message quality (complete fields; low repairs) and route surveillance (out-of-pattern hubs; intermediary profiling).³⁷ From a triangulation perspective, this is significant: multi-hop payments that routinely traverse the same hubs or introduce off-route jurisdictions without clear economic rationale warrant closer review in those corridors highlighted by external evidence.^{12 7 8}

6.5 Where the evidence converges most strongly

Three high-congruence areas emerge. First, gold-linked corridors: external mirror trade anomalies in gold align with supervisory flags on hubs associated with gold aggregation and re-export, strengthening the case for trade-payment congruence testing in these lanes (e.g., value vs. quantity/grade, incoterms, and payment timing).^{12 7}

Second, card/EFT leakage vectors: banks' reports of cash-in followed by foreign cash-out and card-to-crypto/FX pathways dovetail with international typologies on rapid value transformation and quasi-cash usage, implying that scheme-level rules and behavioural analytics are correctly positioned to reduce leakage.^{37 7 8}

Third, advance-payment trades: supervisory emphasis on pre-shipment payments without robust documentary anchors fits TBML patterns of over/under-invoicing and phantom shipments; this argues for selective verification of underlying goods and third-party roles on a risk basis.^{7 8}

6.6 What the triangulation implies for supervisory focus

The combined evidence points to practical priorities for South Africa's risk-based approach. In retail payment rails, continued focus on scheme crypto/quasi-cash controls, geo/velocity limits, and behavioural monitoring (e.g., cash-in then rapid foreign cash-out; bursts of card-not-present spend to newly observed FX/crypto merchants) is well-aligned with the risk patterns banks report.³⁷ For trade-payment lanes, purpose-of-payment validation for advance payments, checks on third-party payer/beneficiary congruence, and targeted sampling of payments linked to price-volatile commodities are appropriate.^{7 8}

In correspondent networks, emphasis on message completeness (Rec.16), low repair incidence, and route analytics (unexpected hubs; repeating intermediary patterns) helps preserve transparency across chains.^{6 38} Given South Africa's macro-trade context and the contribution of goods trade (including gold) to the current account, anchoring these steps in priority corridors is consistent with international assessments and with national external-sector data.^{16 17 18 14 15}

6.7 Towards an analytics blueprint that connects payments to goods

The evidence also supports an analytics blueprint that links payment signals to trade data for targeted lanes. For corridors identified in both datasets, authorities can apply mirror trade and price-band checks (unit values vs. international references), coupled with payment congruence tests (originator/beneficiary roles, third-party presence, payment timing vs. shipping milestones).^{9 12} Filters keyed to advance-payment flags, repeating intermediaries, or rapid value conversion (card to crypto/FX) can prioritise cases. Supervisors can then use correspondent message quality (completeness; low repair; ISO 20022 adoption) to triage cases where data degradation might conceal the originator/beneficiary trail.^{6 38} The resulting model supports iterative targeting: when a lane is validated as higher-risk, expectations on banks' scenario calibration and documentary review can be raised proportionally.³⁷

7. FIC Regulatory Reporting Data

The Financial Intelligence Centre (FIC) analysed regulatory reports – including STRs, SARs, CTRs, TPRs, and IFTRs – received for the period 2022/23 to 2024/25. Using keyword-based data mining, the FIC identified 830 regulatory reports relating to TBML over the three-year review period.^v

Financial Year	Reports	YoY Change
2022/23	145	–
2023/24	338	+133%
2024/25	347	+3%
Total	830	–

Of these 830 reports, 802 (96.6%) were STRs capturing 5,944 transactions valued at approximately R1.43 billion. 27 SARs and 1 STRB were also received. No IFTRs were identified within the TBML-related reporting sample. This may warrant further analysis given the cross-border nature of many TBML typologies.^{vi}

^v Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT.

^{vi} Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT.

- **Reporting by Institution Type** - Cross-border money/value transfer services providers submitted 547 reports (65.9%), banks 217 (26.1%), FX agents 52 (6.3%), and investment advisors 14 (1.7%). Bank-originated reports increased six-fold from 21 in 2022/23 to 124 in 2024/25, likely reflecting improved awareness following SAMLIT engagement and FATF grey-listing reforms.³
- **Reasons for Reporting** - International cash withdrawals account for 76.14% of all TBML-related reports. The remaining 23.86% relate to mis-invoicing (6.39%), misrepresentation of trade activity (2.65%), round-tripping (2.65%), over-invoicing (2.41%), manipulation of bill of lading (1.57%), false valuation (1.45%), structuring (1.45%), and under-invoicing (0.96%).^{vii}
- **Profiles of Reported Individuals and Entities** - Individual profiles show a male-dominant pattern (34% vs. 15% female), with 51–60 age bracket most represented (18%). Nationalities span South Africa, China, India, Pakistan, Nigeria, Kenya, Zimbabwe, DRC, Bulgaria, Cameroon, Fiji, Senegal, Somalia, Sudan, and Uganda. Company profiles: private companies (21%) and close corporations (19%) most frequent, concentrated in Gauteng, KwaZulu-Natal, and Western Cape across wholesale/retail trade, textiles, export, freight, fuel, travel, and foodstuffs.^{viii}

8. Consolidated typologies, red flag indicators, and case studies

The aggregated industry inputs identify the following principal IFF and TBML typologies operating in or through the South African financial system:^{ix}

- **Organised Crime Networks and Syndicate-Driven Flows** - Multiple institutions report exposure to organised crime networks – particularly Chinese syndicates – utilising cross-border EFTs, trade payments, fintech rails, and crypto on/off-ramps. These syndicates employ local intermediaries and operate through layered personal, SME, and mule account structures. Activity is linked to scams, underground banking, and trade mis-invoicing. One documented typology involved illegal wildlife trafficking: a syndicate employed unemployed locals to harvest rare succulent species from Western Cape nature reserves (paying R20–R200 per plant) before selling to international buyers at significantly higher prices.^x
- **Shell Companies and Third-Party Payment Intermediaries** - Shell companies are a pervasive TBML enabler. They are utilised as third-party payment intermediaries to conceal origins of illicit funds, frequently involved in payments for imported commodities where the consignee is not the actual source.
- **Money Laundering via CASPs** - CASPs are rapidly becoming a staple IFF method. Crypto-related transactions (BOP 512/07) account for 56.41% of confirmed cross-border business banking outflows at one institution. The "card-to-crypto" pathway effects near-instant cross-border value transfer. Funds are also routed through legitimate online gambling platforms, exploiting the normal course of business of these intermediaries.^{xi}

vii Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT.

viii Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT.

ix Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025–2026). Confidential – SAMLIT.

x Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025–2026). Confidential – SAMLIT.

xi Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025–2026). Confidential – SAMLIT. Prudential Authority, Aggregated Supervisory Risk-Return Dataset (25 South African Banks, 2023–2025). Confidential – SAMLIT.

- **IFF, TBML and Illegal Wildlife Trade (IWT) convergence** - Environmental crime, particularly IWT, demonstrates clear convergence with the IFF and TBML typologies observed across the South African financial system. Updated analysis by the SAMLIT IWT Task Force confirms that IWT is a form of organised transnational crime – characterised by structured value chains, cross-border financial flows, and deliberate exploitation of legitimate trade routes, business fronts, and payment mechanisms to move and disguise proceeds of crime. Recurring typological features consistent with TBML include the abuse of logistics networks, concealment of illicit commodities such as abalone and rhino horn within commercial consignments, and routing through formal transport corridors – including cross-border trucking routes to landlocked countries – evidencing the use of trade infrastructure as an enabling laundering layer rather than reliance on informal channels alone. The associated financial behaviour mirrors broader IFF indicators observed across other predicate crimes, including structured cash deposits, rapid withdrawals, high-volume low-value transactional patterns, and cross-border transfers following local cash placement. The use of vague or coded transaction references, limited income indicators, and the frequent involvement of couriers or third parties further aligns IWT-related activity with established TBML and organised crime typologies captured in financial sector reporting.
- **Increase in cross-border flows pertaining to the Diamond Sector** - Inbound payments from UAE-based diamond traders—typically reported under BoP categories 101 and 103—are increasingly being used as extended, interest-free advance funding arrangements for the procurement of rough diamonds in South Africa. Although presented as standard commercial pre-payments, these inflows often function in practice as long-duration financing structures (up to 12 months) rather than short-term trade advances. What exacerbates this is the fact that in some instances, the interest-free loans received from UAE based companies are then used to import rough diamonds from the same counterparts in UAE, but the certificate of origin shows South Africa. These arrangements create regulatory and financial-integrity risks, including potential breaches of exchange-control requirements (where foreign-sourced funding constitutes a de facto loan requiring FinSurv approval), potential understated external debt exposure, and misclassification of economic activity in national accounts.^{xii}
- **BOP Code Misuse** - BOP code misuse is a cross-cutting TBML enabler. Codes 401, 101, 102, 103, 200-series, and 289 (management consulting) are frequently misapplied. BOP 289 is highlighted as most abused – it enables cross-border transfers without physical goods, shipping documents, or customs declarations. BOP 109/01 (non-physical exports) also raises risk. In exchange control data, BOP 512 and 289 dominate SARB blocks, with documentation problems triggering 47.83% of blocks.^{xiii}
- **Ponzi-Type and Investment Fraud** - "Pig-butcher" scams employ long-term grooming and legal intimidation. One example: an entity offering loans, bursaries, stokvel, and property investments promised R18,550 returns on R1,000 after 24 months. Red flags include: rapid turnover increases in new accounts; high credit turnover with low balances; absence of salary/tax indicators; repetitive EFT amounts; coded references; no FSCA registration; escalating complaints.^{xiv}

^{xii} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT. FATF, Money laundering and terrorist financing through trade in diamonds (FATF, 2014).

^{xiii} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT. Prudential Authority, Aggregated Supervisory Risk-Return Dataset (25 South African Banks, 2023-2025). Confidential – SAMLIT.

^{xiv} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT.

- **Mule Activity and Networked Fraud** - Mule activity now involves long-standing profiles. Prior scam victims are repurposed as mules. Mule networks have professionalised, including "fund-recovery" services that are part of the fraud ecosystem. Third-party payments/mule activity constitute 44.44% of confirmed personal banking risk events.^{xv}
- **Cash-Intensive Activity with Cross-Border Outflows** - IFF activity increasingly combines cash deposits with rapid externalisation through CASPs or FX channels. FIC data confirms international cash withdrawals as the single largest TBML reporting reason (76.14%). Red flags: large cash deposits followed by rapid FX outflows; cash-to-income ratios 50-100% outside expected profile; geographic inconsistencies in deposit/withdrawal locations.^{xvi}
- **Sanctions Evasion and Governance Abuse** - Emerging evidence shows directors resigning pre-sanctions with non-designated replacements appointed post-sanctions to preserve banking access while maintaining effective control. Red flags: pre-announcement resignations; immediate post-designation appointments; continued banking via historic governance links.^{xvii}
- **Ghost Loans, Identity Theft, and Fraudulent Applications** - Fraudulently originated credit facilities (personal loans, credit cards, overdrafts) via vishing, phishing, and client coaching, with proceeds rapidly dissipated or transferred offshore. Increase in fraudulent home loan applications linked to Zimbabwean nationals with suspected falsified permits.^{xviii}

Red flag indicators:

The following indicators are drawn from all participating institutions, FIC data, and FATF/Egmont typologies:^{xix}

(a) Parties and KYC Context

- Counterparties with limited history, frequent name changes, or shared addresses with unrelated entities.
- Trading in commodities disconnected from known business profile.
- Directors resigning shortly prior to sanctions announcements; new directors appointed immediately post-sanctions.
- Newly registered entities, new-to-bank, making advance payments with no trade history.
- Accounts controlled by third parties (mule accounts). No FSCA registration despite offering investment products.

(b) Documentation and Valuation

- Inconsistencies across invoice, packing list, bill of lading, inspection/insurance certificates; frequent amendments close to payment.
- Unit prices far outside plausible price bands; persistent under-/over-valuation versus partner data.

^{xv} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT.

^{xvi} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT. Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT.

^{xvii} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT.

^{xviii} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT.

^{xix} Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT. Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT. FATF & Egmont Group, Trade-Based Money Laundering: Risk Indicators (FATF, 2020).

- Future-dated bills of lading; unauthorised amendments; interest-free loan advances disguised as trade payments.
- Fraudulent or altered permits; reliance on copies without independent verification.

(c) Shipping and Logistics

- Unusual routes/trans-shipment via hubs with no economic rationale; routing through FTZs obscuring provenance.
- Mismatches between cargo description and shipping mode; inconsistent shipment details vs. Letters of Credit.

(d) Payments and Financial Flows

- Advance payments without documentary anchors; unexplained third-party payers/beneficiaries; split payments across banks.
- Card-not-present bursts to crypto/retail-FX merchants; cash-in followed by rapid foreign cash-out sequences.
- EFT pass-throughs via non-resident FCY accounts; newly opened accounts with rapid turnover increases.
- Repetitive EFT amounts; round transaction values; coded references (e.g., mobile numbers).
- Cash-to-income ratios materially outside expected profile; geographic inconsistencies in deposit/withdrawal locations.
- Misuse of BOP codes 289, 401, 101/01, 109/01, 512/07; circular fund movements through multiple jurisdictions.

(e) Correspondent Chains

- Missing/truncated originator-beneficiary fields; high repair rates.
- Repeated use of unexpected hubs or nested respondents with limited transparency.

Note: These indicators do not prove wrongdoing; they identify cases for review. The strongest signals occur when multiple categories align.

Case Studies

The following case studies illustrate how the typologies, red-flag indicators, and cross-border patterns discussed in Sections 3-8 manifest in practice within the South African financial system. Each case has been anonymised; no institution, customer, or investigation is identifiable. Cases are drawn from aggregated SAMLIT EWG inputs and referrals to the FIC.

Case Study 1: Shell Companies, Cash Structuring, and Illegal Wildlife Trade

Background

Company X, registered in the wholesale trade of food, beverages, and tobacco, was identified through transactional monitoring. Observed account activity was fundamentally inconsistent with the stated business profile and – following review – displayed features consistent with organised money laundering (ML) linked to the Illegal Wildlife Trade (IWT).

Structured cash deposits

The primary account received over R16 million in structured ATM cash deposits, all placed on the same day at ATMs located near South Africa's borders and each carrying the reference "*Wounded Lion*." The deposits bore no connection to declared business activity, the source of funds was unknown, and the ATM location is a recognised IWT-related cash hotspot. The reference itself – combined with the geographic and structuring pattern – strongly indicated links to IWT.

Electronic payments from unrelated entities

The same account also received R24.5 million from Company G, a fuel retailer with no legitimate commercial connection to Company X. Frequent high-value transfers subsequently flowed to and from multiple agent bank accounts, and were directed to three individuals with no identifiable business relationship to the entity.

Secondary account and layering

A secondary account received inbound transfers from a scrap metal company – a sector frequently exploited for Trade-Based Money Laundering (TBML) due to the ease of mispricing. Funds were disposed of through payments to cargo and logistics companies in large round amounts, consistent with the layering and integration stages of ML.

Corroborative evidence – SAMLIT IWT Task Force

Findings from the SAMLIT IWT Task Force reinforce this case and confirm it is not isolated. IWT syndicates routinely exploit registered businesses – including farms, restaurants, logistics providers, air freight operators, and equipment dealers – as fronts to obscure the origin and movement of illicit proceeds. These entities typically display transactional behaviour materially inconsistent with their stated business profiles, including limited business-related expenditure, unexplained third-party payments, and high cash dependence. The Task Force further identifies the involvement of employees, drivers, and couriers in facilitating the movement of both goods and value, with business accounts frequently used absent corresponding commercial activity, and funds layered through withdrawals, remittance services, or cross-border transfers shortly after deposit.

Significance

This case demonstrates the direct intersection between environmental crime and financial crime. Shell companies operating in unrelated industries (fuel, scrap metal, logistics) provided the appearance of legitimate trade while enabling illicit fund flows consistent with IWT-linked laundering. The typologies observed – structured cash deposits, third-party payments, sector-inconsistent activity, and layering through logistics companies – align closely with those documented in broader TBML investigations and reinforce the value of cross-sector monitoring across cash, EFT, and trade-payment rails. The entity was reported to the FIC.

Case Study 2: Illegal Trade in Gold and Tobacco

Background

This case relates to a syndicate that committed fraud and ML through the illegal trade in gold and tobacco – including across the South Africa-Zimbabwe border – together with related tax offences.

Proceeds were laundered with the active assistance of employees at smaller banks, and funds were externalised without authority.

Typology and enablers

The investigation identified clear indicators of professional ML. A legal practitioner assisted in establishing one of the larger laundering schemes, while a separate scheme involved TBML executed through legal persons whose directors are under investigation for third-party and professional ML. Unlicensed Money or Value Transfer Services (MVTs) were used to move large amounts through licensed banking channels, exploiting weaknesses at the correspondent and onboarding layers.

Outcomes

The scheme was disrupted through coordinated action: regulatory and enforcement steps were taken against the implicated banks, and the associated funds were blocked by the Financial Surveillance Department of the South African Reserve Bank (FinSurv). To date, over R240 million has been recovered. The investigation remains ongoing.

Significance

This case illustrates how commodity-linked IFFs – particularly in gold and tobacco – combine cross-border smuggling, professional enablers (legal and banking insiders), and unlicensed MVTs to move value at scale. It reinforces two of the paper's central findings: first, that gold remains a core commodity vulnerability for South Africa; and second, that the integrity of correspondent and onboarding controls at smaller institutions is a material determinant of systemic exposure. It also demonstrates the effectiveness of coordinated public-private action – spanning bank-level supervision, FinSurv blocking powers, and criminal investigation – in disrupting entrenched laundering networks.

9. Joint public-private actions and implementation pathways

9.1 Purpose and framing

This section sets out practical, collaborative actions that the SAMLIT network can advance over the next 12–18 months. The proposals combine (i) what external evidence shows about TBML/IFF patterns (Sections 3–4) with (ii) what South African institutions report in their own risk returns (Section 5) and (iii) where these lenses converge (Section 6). Recommendations are risk-based and proportionate, and they focus on capabilities and coordination rather than directives. ^{6 7 8 12 37 38}

9.2 Cards and EFTs: reducing cross-border leakage on high-velocity rails

The returns highlight three recurring vectors: cash-in, card-out offshore; card-to-crypto/retail-FX; and EFT pass-throughs/third-party payments (often via non-resident foreign currency accounts). To address these jointly, SAMLIT can coordinate:

- Common control baselines across participants. Align on enabling scheme-level crypto/quasi-cash controls, country/MCC geofencing where appropriate, and velocity rules calibrated to patterns observed locally (e.g., cash-in followed by rapid foreign cash-out). Banks already

deploying these controls can share rule heuristics and tuning ranges through SAMLIT technical sessions.³⁷—

- Behavioural analytics library. Translate typologies into feature sets (e.g., cash-in/foreign-cash-out intervals, merchant burst scores for emergent FX/crypto acquirers, SDA utilisation trajectories) and publish as a shared analytics note for participating FIs.^{7 8 37}—
- Purpose-of-payment consistency checks for selected outward EFTs. For advance-payment patterns or third-party beneficiaries, encourage consistent purpose coding, lightweight documentary checks, and exception-based review – with SAMLIT collating what “good” looks like to minimise friction while raising assurance.^{6 7 38}—

9.3 Trade-payment integrity: aligning payments with goods and services

External evidence points to gold and other price-volatile commodities and to corridor concentration; returns emphasise advance-payment and document-light trades. A joint track can:

- Pilot payment-trade congruence testing in priority corridors. For the lanes identified in Section 6, link payment data (timing, third-party roles, route) to trade attributes (declared value/quantity/grade, incoterms). Start with a limited case sample to validate feasibility, then scale.^{12 37}—
- Advance-payment triggers. Develop risk triggers for pre-shipment payments (e.g., unusual price/weight bands, repeated third-party payers, short-cycle circular payments) and share a joint red-flag note through SAMLIT.^{7 8}—
- Document quality signals. Encourage consistent capture of commercial invoice, packing list, and transport document fields that are most diagnostic for TBML (e.g., grade descriptors for precious metals, HS codes prone to misclassification), aligning with FATF/Egmont indicators.^{7 8}—

9.4 Correspondent chains: keeping originator/beneficiary data intact and routes explainable

Given the opacity that can arise across multi-hop payments, the coalition can focus on message quality and route behaviour rather than counterpart-specific judgments:

- Message-quality metrics. Across participating banks, benchmark population of originator/beneficiary elements (Rec.16), repair rates, and free-text reliance; use the Wolfsberg CBDDQ as a common language for expectations with respondents.^{6 38}—
- Route analytics and “unexpected hub” patterns. Establish a simple, privacy-respecting dashboard of repeat intermediary paths, off-route jurisdictions, and chain length outliers in the corridors highlighted in Section 6, with case-based review when patterns persist without clear economic rationale.^{7 8 37}—
- Nested-activity visibility. Where respondents provide services to other FIs/MSBs, align on disclosures and payable-through restrictions consistent with Wolfsberg practices.³⁸—

9.5 Information-sharing, feedback loops, and case uplift

Effective public-private work depends on fast feedback from investigations and structured sharing from banks:

- Typology-to-feature translations. When a case confirms a TBML/IFF pathway (e.g., card-to-crypto, advance-payment phantom shipment, third-party pass-throughs), document the operational breadcrumbs (fields, time lags, sequence) and publish them as machine-readable features for banks to incorporate.^{7 8 37}
- Structured case tags. Encourage common tagging (e.g., ADV_PAY, NR_FCY_PASS, CARD_CNP_CRYPT0) on SARs/STRs and internal alerts to enable cross-institution trend analysis inside SAMLIT.
- Rapid de-confliction lane. For emerging merchant clusters or suspicious intermediary routes, enable a time-bound exchange of minimal indicators among participants, so controls can be tuned consistently without exposing sensitive customer data.

9.6 SARS information requirements and TBML payment-trade linkage

This subsection converts the TBML and IFF typologies discussed in Sections 3–6 into a practical operating model that can be implemented with the South African Revenue Service (SARS). Its main goal is to link cross-border financial activity—such as payments and the use of allowances—to the actual trade transaction, including the declaration, valuation, and physical movement of goods, clearly, auditable, and consistently applied.

SARS (Customs, and where relevant Tax) serves as the primary source of “trade truth,” providing verified information on what was declared, when it occurred, who was involved, and the basis for those declarations. Banks and other authorities complement this by supplying data on payment behaviour, the quality of transaction messaging, and feedback from investigations, helping to create a more complete and effective oversight framework.

Operational outcomes (12–18 months)

- Improve the accuracy of detecting TBML-related value transfers by focusing on cases where payment behaviour does not align with trade declarations (in terms of value, timing, or parties involved).
- Reduce false positives in referrals from banks and public-sector bodies by agreeing on minimum required documentation and standard “mismatch tests” before escalating cases.
- Strengthen revenue protection and compliance by identifying issues such as misclassification (e.g., services vs. goods), post-pricing adjustments, and valuation anomalies, along with their implications for Customs duties, Value-Added Tax (VAT), and income tax.
- Establish a feedback loop where confirmed cases are converted into reusable indicators (such as features, tags, and thresholds), enabling continuous improvement and alignment across all participants.

Minimum SARS information requirements

- Declaration-level data (imports and exports):
Key details from each declaration, including the bill of entry number, release date, customs code, and clearing agent. Also required are the declared Harmonized System (HS) code(s), goods description, quantity and unit of measure, invoice value and currency, and statistical value. Where available, include freight and insurance costs, International Commercial Terms (Incoterms), country of origin, country of consignment or destination, port of entry or exit, transport mode, and shipment references such as container numbers, air waybills, or bills of lading.
- Valuation and amendments:
Information on how goods were valued, including the valuation method and any adjustments (where available). This should also cover post-clearance amendments, tariff or classification changes, and any retrospective debit or credit notes or post-pricing adjustments that affect the customs value. Audit outcomes may be included in aggregated form where appropriate.
- Trader risk context:
Background information on the trader, such as registration status and history, typical trading profile by commodity and trade corridor, and any compliance-related flags that can be shared on a need-to-know basis. Where legally permissible, include ownership or related-party indicators, or links to authoritative sources for beneficial ownership if held outside SARS.
- Trade-statistics context:
Relevant trade statistics from SARS, along with any internal reconciliations or metadata that assist in interpreting commodities that are prone to classification challenges (for example, precious metals).
- Balance of Payments (BOP) service payments, Customs data, and TBML: addressing trade-payment variances
A priority SARS focus area is the investigation of services-related outward payments reported in BOP (including high-volume categories such as BOP 297) where the economic substance appears linked to goods, customs value, or trade terms. In practice, this arises where import-related payments are classified and settled as "services," creating a variance between (i) what is reported on BOP channels, (ii) what is declared to Customs, and (iii) what is disclosed for tax. This variance is consistent with TBML typologies and risk indicators that include trade misinvoicing, misclassification (goods vs services), and post-transaction value adjustments used to shift value across borders after goods have cleared customs.

Why the variance matters:

- Where BOP outward flows increase or persist without a corresponding customs declared trade footprint (or where customs values materially differ from settlement values), this can indicate (i) mis invoicing/over settlement, (ii) unreported imports or phantom trade narratives, (iii) retroactive adjustments not reflected in customs value, or (iv) incorrect classification of payments that obscures the underlying trade event.
- Minimum validation questions: What is being paid for (invoice/contract scope)? Which goods (if any) does it relate to (HS code, entry number, incoterms)? Who are the true parties (payer/beneficiary/related parties)? What is the timing logic (pre shipment, on shipment, post clearance adjustment)? Is the value explainable versus unit price bands and declared customs/statistical values?

- Approvals and controls: Payments Approvals should be assessed against core supporting documents, such as contracts, invoices, and, where services are claimed, evidence that the service was performed. If the transaction relates to goods, it should also be linked to the relevant customs declarations and any valuation adjustments. For higher-risk scenarios (e.g., repeated use of the same third parties, significant post-pricing adjustments, or unusual trade corridors), cases should be escalated based on these risk indicators rather than relying solely on how the payment was coded.

Data sources used in Risk (and how they triangulate)

- BOP data (South African Reserve Bank (SARB) Data): identifies outward payment purpose codes, value, currency, counterparty and corridor; supports detection of service-payment patterns used to settle goods-related obligations, and highlights BOP reporting inconsistencies (e.g., Import bop payments and import-related settlements recorded as services payments, including BOP 297 as observed).
- Customs declaration and valuation data: provides the authoritative trade event (entry, HS code, declared value/quantity/incoterms) and whether any post-clearance amendments or valuation adjustments were declared; enables payment-to-entry congruence and post-price-adjustment validation.
- Advance Payments Notification (APN) data: provides a high-volume risk signal layer that can surface outlier values and behavioural patterns requiring reconciliation to BOP and customs datasets (including investigation of apparent system-driven variances where APN values and SARB downloads diverge).
- Application International Transfer (AIT) data: This data helps identify declared income sources and build a profile of the taxpayer, which should reasonably support their ability to make ongoing outward payments. It also enables risk-based assessment of the plausibility of the "source of funds" or "source of income," particularly where outward payments significantly exceed what would be expected based on reported income or normal trading activity.
- Operationally, variances should be treated as risk selection triggers rather than conclusions. A controlled workflow is to: (i) confirm the integrity of the BOP record (correct code, duplicates, reversals); (ii) establish whether the payment relates to goods, services, or mixed consideration; (iii) link to customs entries; (iv) test value and timing congruence, including whether post price adjustments have been declared to Customs and reflected in relevant tax periods; and (v) determine the appropriate path.

Bulk settlements (including Authorised Dealer with Limited Authority (ADLA)-related structures): transparency constraints and TBML risk

A practical challenge in cross-border monitoring is the use of bulk settlement mechanisms, including structures processed through intermediaries such as ADLAs, where outward or inward payments are only visible as a single aggregated amount. In these cases, banks, regulators and investigators may not have access to transaction-level detail, such as the individual originators, ultimate beneficiaries, or the specific economic purpose of each underlying payment. This lack of transparency can be exploited to conceal TBML related value transfers within otherwise legitimate high-volume settlement flows.

Key risk: When only a bulk settlement is visible, it becomes difficult to identify who is sending funds, whether those originators have a credible source of income, and whether each payment is properly linked to underlying goods or services.

Bulk settlements under BOP 833 used to pay for imports by Authorised Dealers (ADLs)

- Minimum transparency expectations: There should be a defined process through policy, supervision, or targeted information requests to obtain underlying transaction data on a risk basis. This includes originator details, beneficiary or beneficiary institution information (where available), trade corridors, purpose codes, and reference fields that allow linkage to invoices or customs declarations or tax income. Currently transactional level data request in terms of Sect 46 Tax Administration Act (TAA) and Customs Act section 4
- Priority tests: Risk analysis should focus on concentration (e.g., top originators or corridors), unusual value patterns, repeated payments to the same foreign counterparties, signs of circular or “round-tripping” flows, and inconsistencies between originator profiles (including AIT or trading history) and sustained outward settlement activity.

Crypto flows and Crypto Asset Service Provider (CASP)-mediated opacity:

Crypto-asset flows present a distinct transparency challenge: regulators may observe transactions involving a Crypto Asset Service Provider (CASP) without visibility of the ultimate counterparty, wallet holder, or true economic purpose. This is directly relevant to SARS, CASPs, and related data-matching initiatives, as CASP-based structures enable rapid cross-border value movement and layering without the documentary anchors typical of trade transactions. The risk is amplified where CASP activity is funded through cards, Electronic Funds Transfers (EFTs), or bulk settlement arrangements, and where the source of funds, payer identity, and economic purpose are not clearly evidenced.

Potential abuse patterns: repeated funding of CASP accounts followed by rapid conversion or onward transfer; use of intermediaries or mule-like accounts to split transactions below detection thresholds; and use of CASP channels to obscure the true beneficiary in higher-risk corridors.

Triangulation approach: link fiat funding channels (cards, EFTs, bulk settlements) to CASP activity, and test whether the originator profile is plausible against taxpayer income and, where relevant, declared cross-border activity in BOP data. Unexplained inconsistencies should trigger further information requests and be escalated where suspicion thresholds are met.

Controls and data quality focus: ensure complete and consistent payer and purpose information in the fiat funding leg – particularly where bulk settlement codes are used – and apply repeat-pattern monitoring to emerging platforms or merchants not yet captured through static identifiers.

A central governance question is who authorised or enabled the movement of funds. From a tax and IFF perspective, Application International Transfer (AIT) analysis is not limited to comparing declared income with observed flows; it must also assess whether the taxpayer had a credible, explainable capacity to initiate such transfers within existing regulatory, banking, and exchange control frameworks. Where large or repeated CASP-related outflows occur, the concern extends beyond financial mismatch to possible weaknesses in control systems across banks, regulators, and intermediaries – specifically, what checks were performed, what documentation supported the

transaction, and whether the activity was properly risk-assessed rather than processed on surface-level information.

Linking AIT data to CASP activity therefore requires more than timing or affordability checks. The core issue is whether transactions passed through appropriate control points with sufficient scrutiny of source of funds, purpose, and consistency with the taxpayer's known profile. Where CASP flows are permitted despite weak alignment with these factors, this may indicate control bypass, inadequate risk flagging, or gaps at onboarding or transaction review. The risk is heightened where CASP funding grows over time without corresponding growth in declared income, business activity, or tax disclosures – pointing to structural inconsistency rather than isolated anomalies.

Where the gap between AIT-based capacity and observed CASP-related outflows becomes materially large, it should be treated as a structural risk indicator, not a timing issue – reflecting a potential breakdown in preventive controls across the ecosystem, including whether regulators, banks, intermediaries, and CASPs are consistently applying enhanced due diligence and escalating unusual activity. Persistent unexplained variance should trigger coordinated review across tax, exchange control, and financial intelligence functions to determine whether the flows reflect legitimate investment behaviour, underreported income, or deliberate circumvention of controls.

Finally, where fintech-related cross-border flows are processed through bulk settlement structures, the absence of granular transaction-level visibility becomes a key risk factor in its own right – requiring defined mechanisms to access underlying transactional records on a risk basis, rather than reliance on aggregated settlement values.

Payment-trade linkage: matching keys and minimum join logic

- Linking payments to underlying goods transactions is possible even where perfect identifiers are missing, provided a layered matching approach is used. The IFF Risk methodology should apply three levels: (i) direct matching where unique references exist (such as invoice numbers, bill of lading or air waybill, and customs entry numbers); (ii) strong probabilistic matching using stable attributes such as trader identifiers, counterparties, value ranges, currency, and timing windows; and (iii) corridor-level profiling where case-level linkage is not yet possible, based on repeated beneficiaries, consistent trade routes, and recurring intermediaries.
- Primary identifiers (where available): invoice number, purchase order, bill of lading or air waybill, customs entry number, exporter/importer reference fields, and any consistently captured payment purpose references.
- Entity linkage: importer/exporter codes (Customs), company registration or taxpayer reference numbers (Tax), bank customer or account identifiers, and related-party indicators (where lawfully available) to connect group or treasury payments to underlying trade activity.
- Counterparty and corridor linkage: beneficiary name and country, intermediary bank routes (where relevant), country of origin/consignment/destination, port of entry or exit, transport mode, and recurring hub-and-spoke or re-export patterns.
- Value and timing linkage: alignment between payment amounts and declared invoice or statistical values, allowing for tolerances such as partial payments, split shipments, advance payments, and timing windows aligned to key trade events (order, shipment, arrival, and release).

Core TBML congruence tests

- Advance-payment integrity: Identify payments made significantly before shipment or customs release and test whether a corresponding shipment occurs within an expected time window. Escalate cases where no shipment follows (possible phantom trade) or where repeated advance payments do not resolve into completed trade cycles.
- Third-party payer/beneficiary consistency: Flag cases where the payer or beneficiary is not the declared importer, exporter, or contractual counterparty. Assess whether there is a valid explanation, such as documented group treasury arrangements. Repeated third-party patterns in specific corridors or commodities should be prioritised.
- Value congruence (over/under-payment): Compare payment totals to declared customs or statistical values, allowing for legitimate adjustments such as freight, insurance, and Incoterms. Significant deviations may indicate misinvoicing, valuation manipulation, or misclassification between goods and services.
- Unit price / price-band plausibility: Calculate unit values and benchmark them against expected price ranges, adjusted for quality, grade, and trade terms. Persistent deviations, particularly in price-sensitive commodities, should trigger valuation review and potential external benchmarking.
- HS-code and description coherence: Detect frequent HS code changes, mismatches between product descriptions and tariff headings, or use of overly generic descriptions for high-value goods. Prioritise known high-risk classification areas with duty or VAT sensitivity.
- Shipping and route logic: Identify unusual routing patterns, unnecessary trans-shipment through unrelated jurisdictions, or logistics structures that coincide with reduced visibility in payment or trade data.
- Multiple invoicing / split settlement: Detect multiple payments linked to a single invoice or multiple invoices issued for similar goods within tight value and time ranges. Where possible, reconcile against shipment documentation and customs entries.
- Post-price adjustments and Base Erosion and Profit Shifting (BEPS)-linked trade mispricing: Assess whether retrospective adjustments (such as debit notes, royalties, or year-end true-ups) are correctly reflected in customs valuations and tax periods. Mismatches may indicate revenue shifting or TBML layering through services channels.

Information-sharing and governance

- Minimum necessary data: Only share the data required to test a specific hypothesis, such as verifying a shipment linked to an advance payment. Use aggregation where case-level detail is not required.
- Common case tags and structured referrals: Use standardised tags to enable consistent tracking, trend analysis, and control refinement across agencies.
- Closed-loop feedback: When cases are confirmed or dismissed, capture a short outcome note describing what indicators worked or failed (including fields, delays, and thresholds) to improve future detection models.
- Escalation lanes: Define clear pathways for (i) SARS operational action (valuation review, classification correction, audit recovery), (ii) supervisory engagement for systemic control issues, and (iii) referral where suspicion thresholds are met.
- Outputs and measures

- Congruence hit-rate: Share of reviewed cases where payment-trade linkage identifies a confirmed material mismatch in value, timing, party, or routing.
- BOP-Customs variance resolution rate: Proportion of flagged cases resolved into a documented outcome (correction, adjustment, closure, or escalation).
- Revenue protection outcomes: Duties, VAT, and related tax recoveries arising from valuation or classification corrections (tracked separately from enforcement outcomes).
- Bulk settlement transparency yield: Share of bulk settlement alerts where underlying transaction-level data is successfully obtained and enables identification of key originators and beneficiaries.
- CASP linkage yield: Proportion of crypto-related cases where fiat funding can be linked to CASP activity and assessed for source-of-funds plausibility.
- Time-to-triage: Median time from detection to initial decision (close, request information, or escalate).
- Data quality indicators: Availability of usable matching fields (invoice, entry, purpose, payer data) and frequency of missing or inconsistent records affecting linkage.
- Repeat-pattern suppression: Reduction in recurring mismatches for the same trader or corridor following interventions, indicating behavioural or compliance improvement

9.7 Joint public-private implementation pathways

To mitigate TBML at scale, South African Money Laundering and Illicit Trade (SAMLIT), participants should move from ad hoc collaboration to a structured public-private programme that integrates (i) high-velocity payment rail controls, (ii) payment-trade congruence testing, and (iii) targeted, privacy-respecting information exchange. A key insight from TBML enforcement is that the main constraint is often not the identification of typologies, but the operational ability to access relevant data, maintain feedback loops, and execute clear escalation pathways within a legal framework that allows proportionate sharing of minimum necessary information.

Programme governance

- Steering group: Comprising key public agencies and participating financial institutions to set priorities, approve pilot initiatives, and resolve operational or legal barriers (including data access, privacy constraints, and resourcing).
- Four delivery workstreams: (1) Payment rails (cards and EFTs), (2) Trade-payment alignment (Customs-linked analysis), (3) Emerging channels (fintech, bulk settlement, and crypto/CASP), and (4) Legal/policy and safeguards (privacy, data minimisation, and auditability).
- Cadence: Monthly technical working sessions per stream, quarterly steering reviews focused on Key Performance Indicators (KPIs) and escalation outcomes, and an annual refresh of priority corridors and commodities.
- Decision rights: Clear agreement on what constitutes a shared indicator, what requires case-level handling, and which escalation route applies (e.g., supervisory action, SARS intervention, such as a tax review, or referral).

Phased implementation roadmap

1. 0-3 months: Establish the operating model

- Agree priority corridors, commodities, and 3-5 testable TBML hypotheses (e.g., advance payments without shipment, BOP services used to mask goods-related flows, bulk settlement opacity, CASP-funded cross-border transfers).
- Define a minimum shared data dictionary (including required fields, formats, and acceptable tolerances) and ensure the case-tag system is aligned with Section 7.6.
- Establish escalation pathways and standard feedback templates to ensure consistent classification of outcomes (closure, clarification, or escalation).

2. 3-9 months: Run pilots and convert insights into controls

- Pilot payment-trade alignment testing using SARS customs data in selected commodities, focusing on timing, price-band, and third-party mismatch tests.
- Pilot BOP services variance workflows, particularly where goods-related payments are misclassified as services or involve post-price adjustments.
- Test bulk settlement transparency by obtaining underlying transaction-level data on a risk basis and measuring improvement in identifying originators, beneficiaries, and purpose.
- Pilot CASP-related analysis by linking fiat funding to crypto activity and assessing source-of-funds plausibility using taxpayer profiles and AIT data.

3. 9-18 months: Scale, standardise, and embed

- Expand successful pilots across additional corridors and institutions, supported by a standardised “controls and indicators pack” (features, thresholds, and escalation triggers).
- Introduce routine reporting to the steering group, including mismatch heatmaps, corridor risk trends, and resolution outcomes.
- Embed findings into supervisory engagement and industry guidance, focusing on outcomes and minimum control expectations rather than rigid rule-setting.

Legal and policy uplift track

- Strengthen lawful information-sharing frameworks: Ensure existing legal instruments (Memoranda of Understanding (MOUs), regulatory powers, and operating procedures) support proportionate exchange of minimum necessary data for hypothesis testing, with strong audit trails, purpose limitation, and oversight.
- Bulk settlement transparency expectations: Where cross-border flows are processed in aggregated form, establish mechanisms for risk-based access to underlying transaction registers (originator, beneficiary where available, corridor, and purpose references) to prevent TBML concealment within aggregated settlements.
- Payment purpose integrity and documentation standards: Define minimum documentary requirements for high-risk categories (e.g., advance payments, services linked to goods adjustments, bulk settlements crypto), including retention standards to improve auditability and reduce misclassification.
- CASP/fintech visibility enhancements: Review whether current ADLs and CASP-related reporting and recordkeeping is sufficient for source-of-funds, cross-border traceability, and tax consistency checks, and whether additional structured data requirements are needed without undermining legitimate innovation.

- Safeguards by design: Embed privacy, proportionality, and data minimisation principles through indicator-based sharing, time-bound requests, secure handling protocols, and clear retention/disposal rules.

Capability build and sustainability

- Standardise a shared data dictionary and matching logic for payment-trade linkage (including invoice, entry, and tolerance rules for split or partial transactions).
- Maintain a living library of TBML indicators (features, thresholds, and patterns) updated through confirmed case outcomes.
- Conduct joint training and practitioner exchanges covering trade documentation, valuation principles, BOP coding risks, and emerging channels (bulk settlement and CASP/crypto risks).
- Implement periodic assurance testing to validate that controls function as intended and that mismatch detection leads to consistent and repeatable investigative outcomes

10. Conclusion

This report has drawn together three complementary lenses – independent external evidence, aggregated supervisory risk-return data from 25 South African banks, and FIC regulatory reporting – to build a coherent, evidence-based picture of South Africa's exposure to IFF and TBML. Viewed together, these lenses converge on a consistent conclusion: South Africa's exposure is material, cross-border, and multi-channel, concentrated in commodity corridors (most notably gold), high-velocity retail payment rails (cards and electronic funds transfers (EFTs)), and multi-hop correspondent banking chains where originator and beneficiary transparency is most at risk of degradation.

The external evidence – including UNCTAD's mirror-trade findings on non-monetary gold, Global Financial Integrity's country study on trade misinvoicing, and the FATF 2021 Mutual Evaluation Report – establishes the scale and structural nature of the risk. The supervisory returns show *how* value moves through the regulated sector in practice: cash-in followed by foreign cash-out on cards; card-not-present spend to crypto-asset service providers (CASPs) and retail foreign exchange (FX) platforms; EFT pass-throughs and third-party payments (including via non-resident foreign currency accounts); and advance-payment or document-light trade structures.

The jurisdictional clustering reported by banks – the United Arab Emirates, China and Hong Kong, Kenya, Uganda, Pakistan, Nigeria, Mozambique, Zimbabwe, and the Democratic Republic of the Congo – aligns closely with international typologies on commodity hubs, re-export centres, and regional trade corridors. This convergence provides a defensible, risk-based foundation for focusing supervisory attention on payment-trade congruence testing in these lanes, particularly where price-volatile commodities such as gold are implicated.

Cross-cutting structural challenges nonetheless remain. BOP code misuse – particularly codes 289, 512, 101/103, and 833 – continues to obscure the underlying economic substance of cross-border transactions; bulk settlement structures and CASP-mediated flows reduce transparency of originators, beneficiaries, and source of funds; and correspondent chain data quality, nested activity, and route explainability require sustained attention against FATF Recommendation 16 and Wolfsberg baselines. These are not weaknesses unique to any institution or sector; they are systemic features of the modern payments and trade ecosystem that can only be addressed through coordinated action.

Ultimately, disrupting IFF and TBML at scale will depend less on the identification of further typologies – the evidence base is now sufficient – and more on the operational ability of public and private participants to share minimum necessary data lawfully, close feedback loops between confirmed cases and detection features, and align controls across banks, regulators, SARS, SARB, and the FIC. Delivered through the SAMLIT public-private framework set out in Section 9, and reinforced by the recommendations in Section 11, this coordinated response offers a practical, risk-based and regulator-defensible pathway to strengthen South Africa's defences against IFF and TBML, consistent with South Africa's post-delisting sustainability commitments to the FATF and preparations for the next mutual evaluation cycle

11. Recommendations

Recommendations for Financial Institutions:

(a) Cards and EFTs: Reducing Cross-Border Leakage

- Align on common control baselines: scheme-level crypto/quasi-cash controls, country/MCC geofencing, and velocity rules calibrated to local patterns (cash-in followed by rapid foreign cash-out). Share rule heuristics through SAMLIT technical sessions.^{xx}
- Develop a shared behavioural analytics library translating confirmed typologies into feature sets (cash-in/foreign-cash-out intervals, merchant burst scores, SDA utilisation trajectories).
- Implement purpose-of-payment consistency checks for selected outward EFTs, particularly advance payments and third-party beneficiaries.

(b) Trade-Payment Integrity

- Pilot payment-trade congruence testing in priority corridors (China/East Asia, UAE, UK, India, Zimbabwe), linking payment data to trade attributes (value/quantity/grade, Incoterms).^{xxi}
- Develop advance-payment triggers (unusual price/weight bands, repeated third-party payers, short-cycle circular payments) and share through SAMLIT.
- For diamond sector TBML: enhance controls to identify loan-like features in trade transactions; review repayment structures against FinSurv requirements; pursue SADPMR collaboration for a centralised Kimberley Process Certificate registry.^{xxii}

(c) Correspondent Banking

- Benchmark message-quality metrics (Rec. 16 field population, repair rates, free-text reliance) using the Wolfsberg CBDDQ.^{xxiii}

^{xx} Prudential Authority, *Aggregated Supervisory Risk-Return Dataset (25 South African Banks, 2023–2025)*. Confidential – SAMLIT.

^{xxi} FATF & Egmont Group, *Trade-Based Money Laundering: Trends and Developments* (FATF, 2020). UNCTAD, *Trade Misinvoicing in Primary Commodities in Developing Countries* (United Nations, 2016).

^{xxii} *Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025–2026)*. Confidential – SAMLIT. FATF, *Money laundering and terrorist financing through trade in diamonds* (FATF, 2014).

^{xxiii} FATF, *The FATF Recommendations* (FATF, 2012, updated June 2025). Wolfsberg Group, *Correspondent Banking Due Diligence Questionnaire (CBDDQ v1.4) & Principles* (2023).

- Establish route analytics for unexpected hub patterns, off-route jurisdictions, and chain-length outliers with case-based review.
- Enhance nested-activity visibility per Wolfsberg practices for respondents serving other FIIs/MSBs.

(d) Detection and Reporting Enhancement

- Leverage FSCA data to reduce false positives in Ponzi/investment fraud detection.
- Consider conditional debit-restriction mechanisms once a probability threshold is reached for suspected fraud accounts.
- Expand device-level indicators (within privacy-compliant boundaries) to identify mule networks.
- Screen sanctioned entities against CIPC records for former/newly appointed directors; consider historical control and influence.
- Adopt anomaly detection models for open account trade (BOP 101/103) and apply ratio-based cash-to-income monitoring thresholds.

Recommendations for Public Authorities and SAMLIT

- Enhance TBML-specific reporting: Zero IFTRs were filed for TBML during the review period. Develop TBML-specific reporting guidance and training, targeting IFTR use in trade-payment contexts.^{xxiv}
- Publish typology-to-feature translations from confirmed TBML cases as machine-readable features for banks in a secured shared environment and conduct annual refreshes of exposure against noted typologies.
- Introduce structured case tags (ADV_PAY, NR_FCY_PASS, CARD_CNP_CRYPT) on SARs/STRs for cross-institution trend analysis.
- Establish a rapid de-confliction lane for emerging merchant clusters or suspicious intermediary routes.
- Coordinate with SARS Customs on trade-payment congruence pilots, particularly for gold and precious metals.^{xxv}
- Engage SARB/FinSurv on persistent misuse of BOP codes 289 and 109/01, strengthening documentary requirements.
- Track outcome indicators: blocked/reviewed crypto/quasi-cash attempts; advance-payment congruence hit-rates; wire message-completeness trends; TBML-specific STR/IFTR filing rates.^{xxvi}
- Prioritise early notification to regulators for timely preservation orders and asset recovery in Ponzi/investment fraud cases.

^{xxiv} Financial Intelligence Centre, *TBML Data Analysis Findings: Presentation to SAMLIT EWG* (12 February 2026). Confidential – SAMLIT.

^{xxv} UNCTAD, *Trade Misinvoicing in Primary Commodities in Developing Countries* (United Nations, 2016). *Global Financial Integrity, South Africa: Potential Revenue Losses Associated with Trade Misinvoicing (2010-2014)* (GFI, 2018).

^{xxvi} FATF, *Mutual Evaluation Report: South Africa* (FATF, October 2021). FATF, "Jurisdictions under Increased Monitoring" (June 2025); National Treasury, "Statement on FATF Grey-List Delisting" (24 October 2025).

Annexures

Annexure A - Global and regional context (detailed exposition)

Annexure B - Glossary of key terms (public-private usage)

Annexure C - References & Additional Sources

Disclaimer

This publication is intended for information and capacity-building purposes. It does not constitute legal, regulatory, supervisory, or enforcement advice, and it does not attribute wrongdoing to any institution, sector, or jurisdiction. All institutional information drawn from risk returns is aggregated and anonymised; examples are illustrative and do not describe specific customers or cases. External statistics and studies are cited to their original sources; readers should note methodological caveats and the dates of publication. Unless otherwise stated, data and assessments are current as at 18 September 2025. Views expressed are those of the SAMLIT working group and do not necessarily reflect the official positions of any participating institution. Mention of specific standards, tools, or geographies does not imply endorsement or risk ratings.

END OF REPORT

Annexure A — Global and regional context (detailed exposition)

This Annexure sets out the full detail underpinning the high-level summary in Section 3 of the main report.

A.1 Global trends (detailed)

IFFs continue to undermine the stability of the global financial system. While estimates vary depending on methodology, the scale is consistently vast. The UNCTAD suggests that developing countries lose between US\$ 88 and 150 billion annually due to trade misinvoicing¹⁹. Global Financial Integrity has found that in some developing economies IFFs linked to trade misinvoicing may account for as much as 20 per cent of all trade flows²⁰. The International Monetary Fund (IMF) similarly warns that IFFs are not only significant in volume but also destabilising in effect, weakening fiscal capacity, distorting investment flows, and eroding governance²¹.

At the heart of these flows lies TBML, which exploits the immense scale of international trade – worth more than US\$ 32 trillion in goods and services each year²² – to obscure the movement of illicit value. Common TBML methods include over and under-invoicing, multiple invoicing of the same goods, misclassification of goods under incorrect tariff codes, and phantom shipments. These techniques are often supported by falsified documentation such as invoices, bills of lading, and inspection certificates, sometimes facilitated by complicit intermediaries²³. A more detailed explanation of these methods is provided in Annex A (Glossary).

Certain commodities and sectors are especially vulnerable to TBML. Precious metals such as gold and diamonds are attractive due to their high value-to-weight ratio, ease of transport, and opaque trading networks²⁴. Electronics and textiles also feature prominently because their pricing is highly variable and susceptible to manipulation²³. Automobiles and heavy machinery are likewise frequently cited in case studies, with systematic over- or under-invoicing used to justify suspicious cross-border transfers of value²³.

The financial and logistical gateways through which trade is conducted also create vulnerabilities. Free trade zones, of which there are now more than 5 400 worldwide²⁵, provide legitimate trade benefits but often operate with limited customs oversight. This makes them attractive for misinvoicing, document manipulation, and trans-shipment schemes. Similarly, correspondent banking networks – the chains of accounts through which cross-border payments flow – can obscure the identity of the true originator or beneficiary, particularly when multiple intermediaries in different jurisdictions are involved²³.

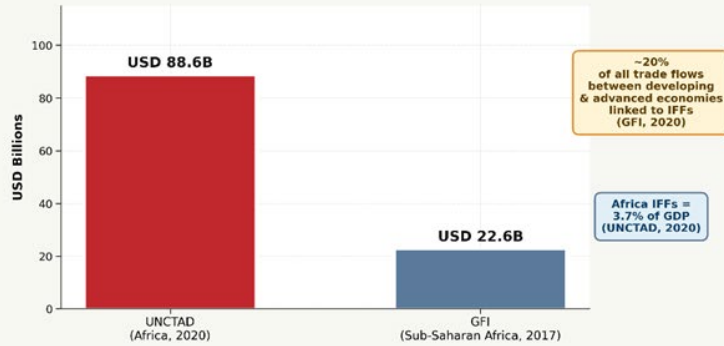
Global typologies published by FATF and the Egmont Group illustrate how these techniques operate in practice. In one case from Latin America, illicitly mined gold was exported using falsified documents and systematically over-invoiced to justify large value transfers, before being re-exported to third countries²³. Another case from Asia documented a textile exporter who consistently under-invoiced shipments to reduce duties while simultaneously over-invoicing imports of raw materials, thereby shifting funds abroad²³. In the Middle East, investigators uncovered phantom shipments where goods were never moved at all. Fabricated documentation was used to justify millions of dollars in cross-border transfers under the guise of legitimate trade²³.

These findings and cases illustrate that TBML is not confined to any one sector or jurisdiction. It is a global problem, adaptive in nature, and increasingly intertwined with other predicate crimes such as drug trafficking, illegal mining, corruption, and tax evasion.

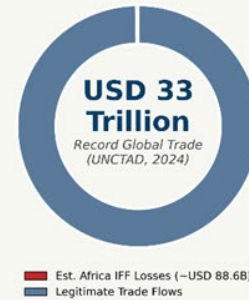
ILLICIT FINANCIAL FLOWS & TRADE-BASED MONEY LAUNDERING

VIEW 1 — Global Trends | Section 3.1

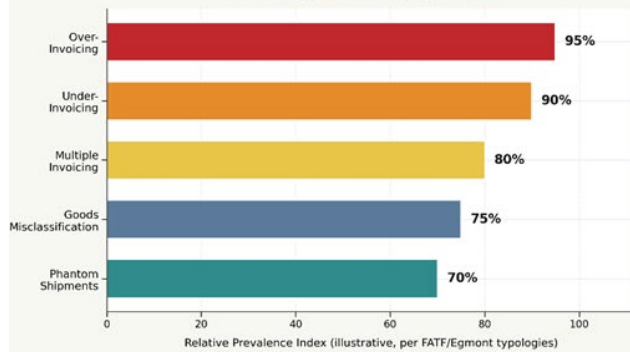
Annual IFF Losses — Africa & Sub-Saharan Africa
(Verified Estimates)



Scale of Global Trade vs Estimated African IFFs



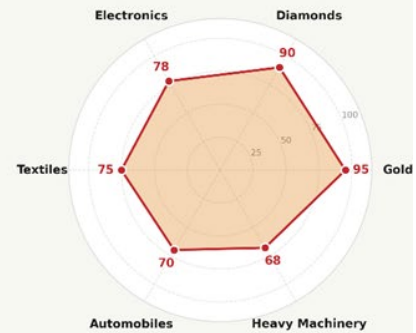
Common TBML Techniques
(FATF / Egmont Group Typologies)



Sources: UNCTAD (2020, 2023) · GFI (2020) · IMF · FATF / Egmont Group Typologies · WTO Trade Statistics

Note: Prevalence indices and commodity risk scores are illustrative, derived from relative emphasis in FATF/Egmont typology reports.

Commodity Vulnerability to TBML
(Illustrative Risk Scores)

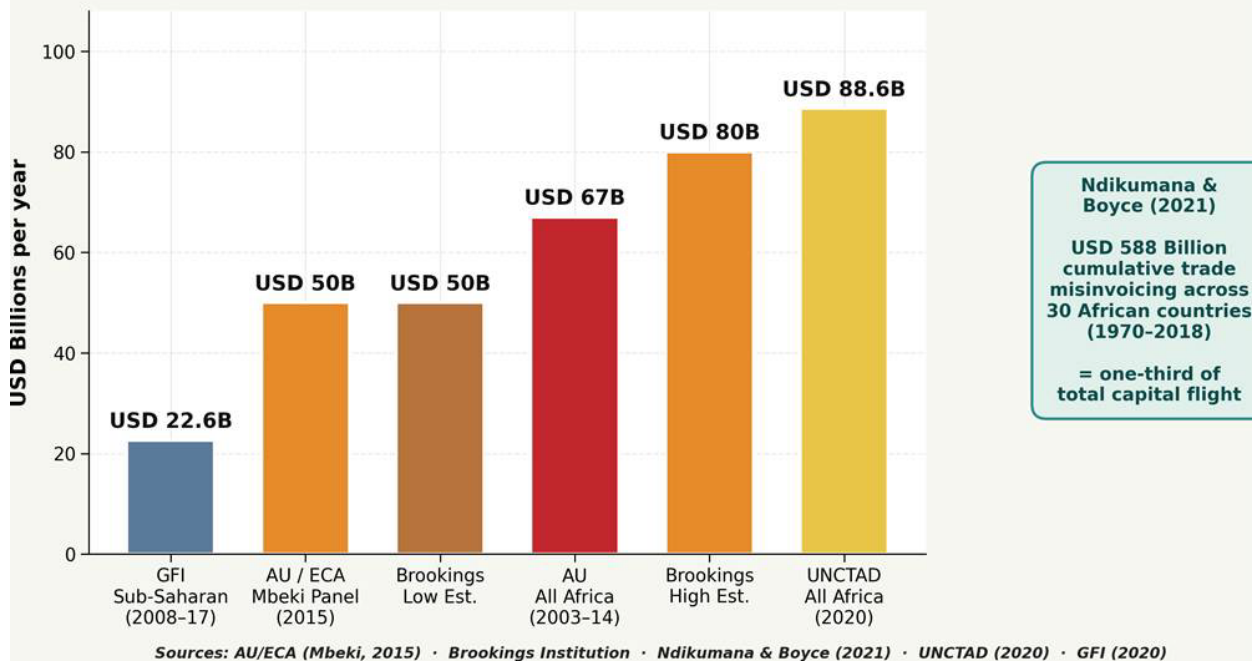


A.2 Regional African trends (detailed)

Africa is disproportionately affected by IFFs relative to the size of its economy. The African Union and the United Nations Economic Commission for Africa, through the High-Level Panel on Illicit Financial Flows chaired by former South African President Thabo Mbeki, estimated in its 2015 report that more than US\$ 50 billion was being lost annually from the continent through such flows. While this estimate is now a decade old, subsequent studies (including UNCTAD 2020 and GFI 2021) confirm that the order of magnitude remains materially unchanged.²⁶ The Brookings Institution places this figure even higher, suggesting that IFFs deprive African governments of US\$ 50-80 billion each year²⁷ in foregone revenues. Complementing these findings, Ndikumana and Boyce calculated that net trade misinvoicing across 30 African countries between 1970 and 2018 amounted to US\$ 588 billion, representing nearly a third of total capital flight from the 54-country continent.²⁸

ILLICIT FINANCIAL FLOWS FROM AFRICA

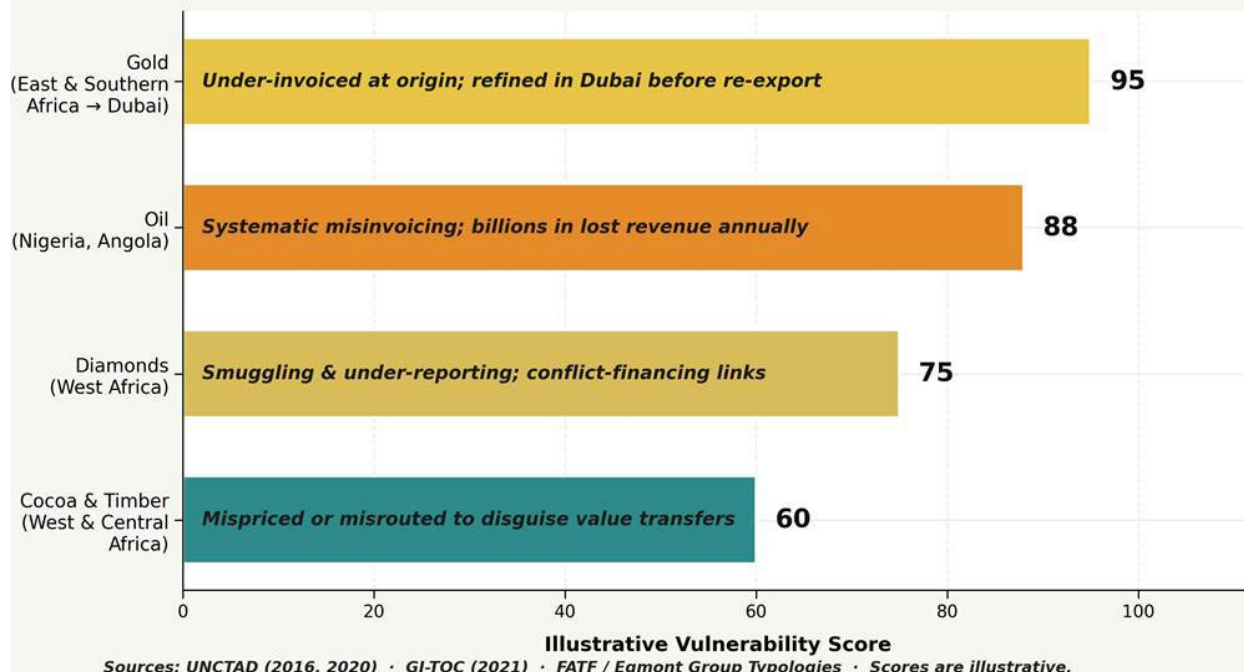
Annual IFF Loss Estimates Across Authoritative Sources | Section 3.2



Commodities play a central role in Africa's vulnerability to IFFs. Gold is particularly significant: Reports by UNCTAD and the Global Initiative Against Transnational Organized Crime highlight large-scale under-invoicing of gold exports in East and Southern Africa²⁹. Much of this gold is routed through Dubai, where it is refined or re-classified before being re-exported²⁹. Oil exports from countries such as Nigeria and Angola have also been subject to systematic misinvoicing, costing governments billions in lost revenue each year³⁰. Diamonds in West Africa continue to present risks of smuggling and under-reporting, sometimes linked to conflict financing³¹. Even agricultural commodities, such as cocoa in West Africa and timber in Central Africa, have been mispriced or misrouted to disguise value transfers³².

AFRICAN COMMODITY VULNERABILITIES TO TBML

Illustrative Vulnerability Scores per UNCTAD, GI-TOC and FATF | Section 3.2



Several geographic hubs have emerged as focal points for TBML schemes. Dubai has become a major destination for African gold, particularly where exports are under-declared at origin²⁹. Nairobi and Dar es Salaam are important re-export hubs where goods may be misclassified or subject to phantom shipping practices³³. Johannesburg, as southern Africa's commercial and financial centre, functions as a legitimate trade hub but is also exposed as a potential laundering node where financial-institution, customs and exchange-control oversight is inconsistently applied – for example, where trade documentation is not independently verified against payment flows, or where beneficial ownership of counterparties is not fully established at onboarding. . Mauritius, with its free trade zones and reputation for corporate secrecy, has also been highlighted by UNCTAD as a jurisdiction

GEOGRAPHIC TBML HUBS — AFRICA & KEY CORRIDORS

Focal points where trade-based laundering schemes concentrate | Section 3.2

Dubai (UAE)

Major destination for African gold — exports under-declared at origin, refined or re-classified, then re-exported to global markets.

Nairobi & Dar es Salaam

Important re-export hubs where goods may be misclassified or subject to phantom shipping practices.

Johannesburg

Southern Africa's commercial & financial centre — a legitimate trade hub also exposed as a laundering node where FI, customs & exchange-control oversight is inconsistently applied.

Mauritius

Free trade zones and reputation for corporate secrecy — highlighted by UNCTAD as vulnerable to trade-based value transfer.

Hong Kong

Key corridor for commodity flows from Africa — repeatedly cited in global and regional TBML studies.

Sources: UNCTAD (2016, 2020) · GI-TOC (2021) · FATF / Egmont Group

These vulnerabilities are compounded by structural challenges across much of the continent. Customs and revenue authorities (which hold declaration- and invoice-level trade data) and financial intelligence units (which receive suspicious transaction and cross-border payment reports) often operate on separate data platforms, limiting their combined ability to detect misinvoicing in real time. Effective detection depends on structured information-sharing pathways between revenue authorities, FIUs and supervisors, rather than on any single institution holding all relevant records³⁵. Many customs administrations lack the tools for mirror trade analysis or systematic price band checks. High levels of informality in cross-border trade encourage the use of informal value transfer systems, which can bypass the regulated sector entirely³⁵. Finally, governance risks such as corruption within customs and border agencies can undermine enforcement efforts³⁶.

STRUCTURAL CHALLENGES COMPOUNDING AFRICA'S TBML VULNERABILITY

Enforcement, data, informality and governance barriers | Section 3.2

Data Integration Gaps

Customs & revenue authorities (holding invoice-level trade data) and FIUs (receiving STRs and cross-border payment reports) often operate on separate data platforms — limiting combined ability to detect misinvoicing in real time.

Weak Analytical Capacity

Many customs administrations lack the tools for mirror-trade analysis or systematic price-band checks.

High Informality in Cross-Border Trade

High levels of informality encourage the use of informal value transfer systems, which can bypass the regulated sector entirely.

Governance & Corruption Risks

Corruption within customs and border agencies can undermine enforcement efforts, allowing TBML to persist unchecked.

Sources: UNCTAD (2016, 2020) · FATF / Egmont Group · Mbeki Panel (2015)

Concrete cases illustrate these dynamics. In Tanzania, authorities uncovered widespread under-declaration of gold exports, with billions in tax revenues lost and shipments ultimately re-routed through Dubai³³. In Nigeria, studies revealed persistent discrepancies between official oil export values and partner country import records, pointing to systematic TBML practices³⁰. In West Africa, cocoa and timber exports have been under-invoiced or diverted through third countries, further demonstrating how agricultural products are exploited for IFFs³².

A.3 Implications for South Africa (detailed)

The global and regional evidence makes clear that South Africa cannot view TBML as a distant or external phenomenon. The country is both a significant exporter of commodities — particularly gold and other precious metals — and a regional financial hub with extensive trade linkages across Africa and beyond. The vulnerabilities identified globally, such as misinvoicing of high-value commodities and the misuse of financial gateways, align closely with South Africa's trade profile.

Moreover, the corridors repeatedly highlighted in global and regional studies — such as flows to Dubai, Hong Kong, and regional African partners including Mozambique and Kenya — are directly relevant to South Africa's trade patterns. Structural challenges observed elsewhere in Africa, such as limited integration between customs and financial intelligence or weak application of mirror trade analytics, also resonate with South Africa's current supervisory and enforcement environment.

This broader context underscores why South Africa's exposure to TBML and related IFFs must be understood in both global and regional terms. It also sets the foundation for Section 4 of this report, which examines the country's exposure using external evidence, and Section 5, which analyses supervisory insights drawn from bank risk returns.

IMPLICATIONS FOR SOUTH AFRICA

Why global and regional TBML trends matter domestically | Section 3.3

Commodity Exposure

South Africa is a significant exporter of gold and other precious metals — the very commodities identified as most vulnerable to TBML globally and regionally.

Trade Corridor Alignment

Key corridors repeatedly highlighted — Dubai, Hong Kong, and regional partners including Mozambique and Kenya — are directly relevant to SA's trade patterns.

Regional Financial Hub Risk

Johannesburg — Southern Africa's commercial & financial centre — is both a legitimate trade hub and a potential laundering node where controls are weak.

Supervisory & Enforcement Gaps

Limited integration between customs and financial intelligence, and weak application of mirror-trade analytics, resonate with SA's supervisory environment.

Sources: UNCTAD (2016, 2020) · GFI (2018) · FATF MER South Africa (2021)

Annexure B Glossary of key terms (public–private usage)

- Illicit Financial Flows (IFFs). Cross-border movements of money, capital or value that are illegal in source, transfer, or use, or that are purposefully concealed to evade laws, taxes, or regulations. In this report, the focus is on commercial IFFs driven by mispricing, fictitious trade, or misuse of payment rails (cards/EFTs).⁽¹²⁾
- Trade-Based Money Laundering (TBML). The process of disguising the proceeds of crime and moving value through trade transactions to legitimise their illicit origin. TBML leverages the complexity and volume of trade, exploiting documentation, valuation, and logistics to obscure ownership and value transfer.⁽⁷⁾⁽⁸⁾
- Over/Under-invoicing. Manipulating the price of goods or services on invoices relative to arm's-length values to move value across borders. Over-invoicing shifts value out (payer overpays); under-invoicing shifts value in (payer underpays).⁽⁷⁾
- Multiple invoicing. Issuing more than one invoice for the same shipment to justify multiple payments, often through different financial institutions.⁽⁷⁾
- Misclassification / HS-code abuse. Declaring goods under incorrect tariff codes to affect duties, risk controls, or statistical visibility (e.g., labelling high-value goods as low-value components).⁽⁷⁾
- Phantom shipments. Recording exports/imports that did not occur, or materially inflating quantities/grades, with falsified documents to justify payments.⁽⁷⁾
- Advance payment. Payment before shipment/inspection. Legitimate in commerce, but a higher-risk TBML structure when documentation is weak, counterparties are opaque, or the payment cycles back via third parties.⁽⁷⁾⁽⁸⁾
- Third-party payer or beneficiary. An entity not party to the underlying sale or purchase sends or receives the funds. May be legitimate (e.g., group treasury), but is a TBML red flag when unexplained, repetitive, or route-incongruent.⁽⁷⁾
- EFT . Account-to-account payments (domestic or cross-border). Here, we focus on EFTs used to pass value through third parties or non-resident foreign currency accounts without clear economic purpose.⁽³⁷⁾
- Debit/Credit card cross-border usage. Card rails used for foreign ATM cash-outs, card-not-present spending at crypto/retail-FX merchants, or rapid offshore spend following local cash-in. Requires rule-based and behavioural controls.⁽³⁷⁾
- MCC (Merchant Category Code). Scheme-assigned merchant taxonomy used for rules/filters (e.g., "quasi-cash", crypto indicators) in card monitoring.⁽³⁷⁾
- Non-resident foreign-currency (FCY) account. Accounts held by non-residents in foreign currency at a South African bank. Legitimate use exists, but pass-through patterns (non-resident↔non-resident) with no SA footprint elevate risk.⁽³⁷⁾
- Single Discretionary Allowance (SDA). South African exchange-control personal allowance. Banks monitor SDA utilisation patterns for card/EFT behaviours linked to cross-border leakage.⁽³⁷⁾
- Correspondent banking / Nostro-Vostro. Bank-to-bank relationships enabling cross-border payments via multi-hop chains. Transparency depends on message quality and visibility into nested activity.⁽⁶⁾⁽³⁸⁾

- Travel rule (FATF Rec.16). Requirement that complete and accurate originator/beneficiary information accompany wire transfers, end-to-end, across correspondent chains.⁽⁶⁾
- Mirror trade analysis. Comparing a country's declared exports/imports with partner-country declarations to detect systematic gaps suggestive of misinvoicing.⁽¹²⁾
- Price-band checks. Comparing unit values declared in trade with reference price bands for the commodity, adjusted for quality/grade and Incoterms.⁽⁹⁾
- Free Trade Zone (FTZ). Special zones with customs/tax incentives. Legitimate benefits, but heightened TBML exposure when oversight is light and trans-shipment/document manipulation are common.⁽⁷⁾

Annexure C – References & Additional Sources

References

- [1] United Nations Statistics Division / UNCTAD / UNODC (2022). Conceptual Framework for the Statistical Measurement of Illicit Financial Flows. Background Document for the 53rd Session of the UN Statistical Commission. <https://unstats.un.org/unsd/statcom/53rd-session/documents/BG-3j-Crime&CriminalJusticeStats-II-E.pdf>
- [2] Financial Action Task Force (FATF) & Egmont Group (2020). Trade-Based Money Laundering: Trends and Developments. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf>
- [3] United Nations Conference on Trade and Development (UNCTAD) (2025). SDG Pulse 2025: Statistical Report. Geneva: UNCTAD. https://unctad.org/system/files/official-document/stat2025d2_en.pdf
- [4] Global Financial Integrity (2018). South Africa: Potential Revenue Losses Associated with Trade Misinvoicing (2010–2014). Executive Summary & Report. <https://gfin integrity.org/wp-content/uploads/2018/11/South-Africa-Report-2018-Executive-Summary.pdf>
- [6] Financial Action Task Force (FATF) (2012, updated June 2025). The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>
- [7] FATF & Egmont Group (2020). Trade-Based Money Laundering: Trends and Developments. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf>
- [8] FATF & Egmont Group (2020). Trade-Based Money Laundering: Risk Indicators. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Risk-Indicators.pdf>
- [9] UNCTAD & UNODC (2023). Statistical Measurement of Tax and Commercial Illicit Financial Flows: Pilot testing methodologies for SDG indicator 16.4.1. https://unctad.org/system/files/official-document/stat2023d1_en.pdf
- [12] UNCTAD (2016). Trade Misinvoicing in Primary Commodities in Developing Countries: The cases of Chile, Côte d'Ivoire, Nigeria, South Africa and Zambia. https://unctad.org/system/files/official-document/suc2016d2_en.pdf
- [14] FATF (2021). Mutual Evaluation Report – South Africa. <https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-South-Africa.pdf>
- [15] FATF (13 June 2025). Jurisdictions under Increased Monitoring (“Grey list”). <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-june-2025.html>
- [16] World Bank (WDI). Exports and Imports of goods and services (% of GDP) – South Africa (latest available). <https://databank.worldbank.org/reports.aspx?country=ZAF&source=2>
- [17] South African Revenue Service (31 Jan 2025). Trade Statistics for December 2024. <https://www.sars.gov.za/media-release/trade-statistics-for-december-2024/>
- [18] South African Reserve Bank (June 2025). Quarterly Bulletin – June 2025. <https://www.resbank.co.za/en/home/publications/publication-detail-pages/quarterly-bulletins/quarterly-bulletin-publications/2025/june>
- [19] UNCTAD (2020). Economic Development in Africa Report 2020: Tackling Illicit Financial Flows for Sustainable Development in Africa. <https://unctad.org/publication/economic-development-africa-report-2020>

- [20] Global Financial Integrity (2021). Illicit Financial Flows to and from 135 Developing Countries: 2009–2018. <https://gfin integrity.org/wp-content/uploads/2021/12/IFF-Report-2021.pdf>
- [21] International Monetary Fund (2023). The IMF and the Fight Against Illicit Financial Flows (Factsheet). <https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-illicit-financial-flows>
- [22] UNCTAD (13 Dec 2022). Global trade set to hit record \$32 trillion in 2022. <https://unctad.org/news/global-trade-set-hit-record-32-trillion-2022-outlook-increasingly-gloomy-2023>
- [23] FATF/Egmont (2020). TBML: Trends and Developments & TBML: Risk Indicators. <https://www.fatf-gafi.org/en/publications/Methodsand trends/Trade-based-money-laundering-trends-and-developments.html>
- [24] Global Initiative Against Transnational Organized Crime (2021). Illicit Gold Markets in East and Southern Africa. <https://globalinitiative.net/wp-content/uploads/2021/05/Illicit-gold-markets-in-East-and-Southern-Africa-GITOC-.pdf>
- [25] UNCTAD (2019). World Investment Report 2019 – Special Economic Zones. https://unctad.org/system/files/official-document/wir2019_en.pdf
- [26] African Union/UNECA (2015). Report of the High Level Panel on Illicit Financial Flows from Africa (Mbeki Report). https://au.int/sites/default/files/documents/40545-doc-IFF_REPORT.pdf
- [27] Brookings Institution (2020). Illicit financial flows in Africa: Drivers, destinations, and policy options. <https://www.brookings.edu/wp-content/uploads/2020/02/Illicit-financial-flows-in-Africa.pdf>
- [28] Ndikumana, L. & Boyce, J. (2021). Capital Flight from Africa, 1970–2018: New Estimates. PERI, University of Massachusetts. <https://peri.umass.edu/wp-content/uploads/2025/01/CapFlightAfrica-5-28-21.pdf>
- [29] GI-TOC (2021) and UNCTAD (2016) on African gold flows via Dubai; see sources above. <https://globalinitiative.net/analysis/illicit-gold-east-southern-africa/>
- [30] Global Financial Integrity (2018). Nigeria: Potential Revenue Losses Associated with Trade Misinvoicing. <https://gfin integrity.org/wp-content/uploads/2018/10/Nigeria-Report-2018.pdf>
- [31] FATF (2014). Money laundering and terrorist financing through trade in diamonds. <https://www.fatf-gafi.org/en/publications/Typologies/typologies-reports.html>
- [32] UNCTAD (2016). Trade misinvoicing in primary commodities (incl. agricultural products). <https://unctad.org/publication/trade-misinvoicing-primary-commodities-developing-countries>
- [33] GI-TOC (2021). Illicit gold markets in East and Southern Africa (hubs such as Nairobi and Dar es Salaam). <https://globalinitiative.net/analysis/illicit-gold-east-southern-africa/>
- [34] UNCTAD (2019). World Investment Report 2019 – Special Economic Zones (FTZ risks, incl. Mauritius context). https://unctad.org/system/files/official-document/wir2019_overview_en.pdf
- [35] UNCTAD/UNODC (2021–2023). Methodological guidelines & pilot results for SDG 16.4.1 measurement. https://unctad.org/system/files/non-official-document/20210917_IFFGuidelinesForPilots_en_0.pdf
- [36] Transparency International (2024). Corruption Perceptions Index 2023/2024. <https://www.transparency.org/en/cpi>
- [37] SAMLIT Working Group (2025). Aggregated supervisory risk-return dataset (25 South African banks, 2023–2025). Internal supervisory data aggregated for public reporting.
- [38] Wolfsberg Group (2023). Correspondent Banking Due Diligence Questionnaire (CBDDQ v1.4) & Principles. <https://wolfsberg-group.org/resources/>

The following sources are cited in the roman numeral footnotes throughout the EWG report:

International and Multilateral Sources

- African Union/UNECA, Report of the High Level Panel on Illicit Financial Flows from Africa (2015). https://au.int/sites/default/files/documents/40545-doc-IFFs_REPORT.pdf
- Brookings Institution, "Illicit financial flows in Africa: Drivers, destinations, and policy options" (2020). <https://www.brookings.edu/wp-content/uploads/2020/02/Illicit-financial-flows-in-Africa.pdf>
- FATF, Mutual Evaluation Report: South Africa (October 2021). <https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-South-Africa.pdf>
- FATF, "Jurisdictions under Increased Monitoring" (updated June 2025). <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-june-2025.html>
- FATF, The FATF Recommendations (2012, updated June 2025). <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf>
- FATF, Money laundering and terrorist financing through trade in diamonds (2014). <https://www.fatf-gafi.org/en/publications/Typologies/typologies-reports.html>
- FATF & Egmont Group, Trade-Based Money Laundering: Trends and Developments (2020). <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf>
- FATF & Egmont Group, Trade-Based Money Laundering: Risk Indicators (2020). <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Risk-Indicators.pdf>
- Global Financial Integrity, South Africa: Potential Revenue Losses Associated with Trade Misinvoicing (2010-2014) (2018). <https://gfintegrity.org/wp-content/uploads/2018/11/South-Africa-Report-2018-Executive-Summary.pdf>
- Global Initiative Against Transnational Organized Crime, Illicit Gold Markets in East and Southern Africa (2021). <https://globalinitiative.net/wp-content/uploads/2021/05/Illicit-gold-markets-in-East-and-Southern-Africa-GITOC-.pdf>
- International Monetary Fund, "The IMF and the Fight Against Illicit Financial Flows" (Factsheet, 2023). <https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-illicit-financial-flows>
- L Ndikumana & J Boyce, Capital Flight from Africa, 1970-2018: New Estimates (PERI, UMass, 2021). <https://peri.umass.edu/wp-content/uploads/2025/01/CapFlightAfrica-5-28-21.pdf>
- UNCTAD, Economic Development in Africa Report 2020: Tackling Illicit Financial Flows (2020). <https://unctad.org/publication/economic-development-africa-report-2020>
- UNCTAD, Trade Misinvoicing in Primary Commodities in Developing Countries (2016). https://unctad.org/system/files/official-document/suc2016d2_en.pdf
- UNCTAD, "Global trade set to hit record \$32 trillion in 2022" (13 December 2022). <https://unctad.org/news/global-trade-set-hit-record-32-trillion-2022>
- UNCTAD & UNODC, Statistical Measurement of Tax and Commercial IFFs: Pilot testing for SDG 16.4.1 (2023). https://unctad.org/system/files/official-document/stat2023d1_en.pdf
- Wolfsberg Group, CBDDQ v1.4 & Principles (2023). <https://wolfsberg-group.org/resources/>
- World Bank (WDI), Exports/Imports of goods and services (% GDP) – South Africa.

South African Sources

- Financial Intelligence Centre, TBML Data Analysis Findings: Presentation to SAMLIT EWG (12 February 2026). Confidential – SAMLIT.
- National Treasury, "Statement on FATF Grey-List Delisting" (24 October 2025).
- South African Reserve Bank, Quarterly Bulletin – June 2025. <https://www.resbank.co.za/en/home/publications/publication-detail-pages/quarterly-bulletins/quarterly-bulletin-publications/2025/june>

- South African Revenue Service, Trade Statistics for December 2024 (31 January 2025). <https://www.sars.gov.za/media-release/trade-statistics-for-december-2024/>

SAMLIT Internal Sources (Confidential)

- Aggregated anonymised industry input, SAMLIT IFF and TBML Expert Working Group (2025-2026). Confidential – SAMLIT.
- Prudential Authority, Aggregated Supervisory Risk-Return Dataset (25 South African Banks, 2023-2025). Confidential – SAMLIT.
- SAMLIT IFF and TBML EWG, Trade Finance Product Typology Working Paper (2025). Confidential – SAMLIT.