Enhancing Private-Private Information Sharing in South Africa to Disrupt Economic Crime

E Matthee*, A van Zyl** and P Steenkamp***

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Authors

Elzé Matthee
Albert van Zyl
Philip Steenkamp

Affiliation

North-West University, South Africa

Email

elzematthee@gmail.com
albert.vanzyl@nwu.ac.za
philip.steenkamp@nwu.ac.za

Date Submitted

16 February 2026

Date Revised

23 October 2026

Date Accepted

23 October 2026

Date Published

05 November 2026

Guest Editor

Prof Jacqui-Lyn McIntyre

Journal Editor

Prof Wian Erlank

How to cite this contribution

Matthee E, Van Zyl A, Steenkamp P "Enhancing Private-Private Information Sharing in South Africa to Disrupt Economic Crime" *PER / PELJ* 2026(29) - DOI https://dx.doi.org/10.17159/1727-3781/2026/v29i0a25824

Copyright

DOI
https://dx.doi.org/10.17159/1727-3781/2026/v29i0a25824

Abstract

Purpose – Economic crime continues to evolve globally, demanding greater sophistication and collaboration for the better prevention, detection and disruption thereof. This paper examines the need for and status of South African (SA) private-private information sharing (P2P) as an intervention by comparing the *Draft Amendments to the Money Laundering and Terrorist Financing Control Regulations* (the *Draft Amendments*) aimed at regulating information sharing between accountable institutions to selected international counterparts to enhance the country's capacity for P2P.

Design/methodology/approach – After identifying the purpose of P2P, a comparative analysis using secondary data was conducted of key aspects of the proposed P2P framework against the selected international P2Ps, from the USA, Singapore, the Netherlands and Estonia.

Findings – A legally sound, secure and efficient P2P that leverages resources and information from a wide range of private sector stakeholders is essential for enhancing the effectiveness of measures aimed at disrupting economic crime. Legislative amendments have opened the door for an SA P2P framework, but the detailed embodiment thereof is still lacking. The proposed P2P framework compares favourably with equivalent international frameworks. It is recommended that the participation, effectiveness and ambit thereof be enhanced, not only for the next round of FATF mutual evaluations but also to bolster South Africa's ability to disrupt economic crime.

Originality/Value – South Africa formally introduced P2P in 2022 with the enactment of section 41A(3) of *FICA*, followed by its envisioned embodiment as outlined in the *Draft Amendments*. Limited research has been conducted on the concept of P2P and the proposed SA framework. This article aims to support the development of a SA P2P framework, provide clarity to private sector entities to support the concept, and contribute to its effectiveness and efficiency.

Research limitations – The availability of information was limited due to the nature of P2P frameworks and the novelty of the concept.

Article type – Individualising comparative analysis

Keywords

AML Bridge; COSMIC; economic crime; *PATRIOT Act*; private-private information sharing; South Africa; TMNL.

1 Introduction

South Africa is grappling with significant economic crime,[1] as evidenced by its 2023 Financial Action Task Force (FATF) greylisting,[2] rampant corruption and state capture, public procurement fraud, and record-setting corporate and crypto-based failures.[3] Numerous indices, such as the 2025 Secretariat Economic Crime Index (SECI) – which leverages the Organized Crime Index,[4] the Transparency International Corruption Perception Index,[5] and the Basel Anti-Money Laundering (AML) Index[6] – reflect this troubling reality. According to the SECI, the country exhibits weak anti-crime frameworks, substantial regulatory gaps, and a high prevalence of high-risk activities.[7] The Basel AML Index indicates that countries with a high risk of money laundering and terrorist financing (ML/TF) – both types of economic crime – share several characteristics: weak public institutions, inadequate political rights and rule of law; insufficient resources to oversee the financial system; a predominant cash-based economy; restrictions on press

* Elzé Matthee. BCom, BCom Honours, and MCom in Forensic Accountancy, School of Accounting Sciences, Faculty of Economic and Management Sciences, North-West University, South Africa. E-mail: elzematthee@gmail.com. ORCiD: https://orcid.org/0009-0009-0484-5506.

** Albert van Zyl. BCom Law, LLB and LLM. North-West University Business School, Faculty of Economic and Management Sciences, North-West University, South Africa. E-mail: albert.vanzyl@nwu.ac.za. ORCiD: https://orcid.org/0000-0003-1095-2614.

*** Philip Steenkamp. LLB, LLM and Doctorate in Risk Management. School of Accounting Sciences, Faculty of Economic and Management Sciences, North-West University, South Africa. E-mail: philip.steenkamp@nwu.ac.za. ORCiD: https://orcid.org/0000-0002-3644-9446.

1 Defined as "illegal acts committed by an individual or a group of individuals to obtain a financial or professional advantage" (Europol 2025 https://www.europol.europa.eu/crime-areas/economic-crime; Swanepoel *Financial and Moral Perspective* 2.)

2 The Financial Action Task Force (FATF) removed South Africa from the greylist on 24 October 2025.

3 Such as Steinhoff, Tongaat Hulett, and Mirror Trading International.

4 Global Initiative Against Transnational Organized Crime 2023 https://ocindex.net/report/2023/0-3-contents.html.

5 Transparency International 2024 https://images.transparencycdn.org/images/CPI2024_Report_Eng1.pdf.

6 Mkhabela "South Africa and the Capture of the Executive" 119; FATF 2023 https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html; Basel Institute on Governance 2024 https://baselgovernance.org/sites/default/files/2024-11/2024%20Basel%20AML%20Index%20report.pdf.

7 Secretariat 2025 https://secretariat-intl.com/wp-content/uploads/2025/04/Secretariat-Global-Financial-and-Economic-Crime-Outlook-2025.pdf.

freedom; low levels of financial or political transparency; and elevated levels of illegal smuggling and trafficking (e.g., drugs, humans, wildlife).[8]

The situation is exacerbated internationally, as the disruption of economic crime becomes increasingly challenging due to the evolving sophistication and resources of perpetrators.[9] This evolution is driven by technological advancements (e.g., crypto assets, cloud computing, social media and artificial evidence), flexible digital instant payment mechanisms and interconnected financial systems,[10] alongside the activities of criminal networks.[11] The siloed operations and restricted access to real-time information resulting from insufficient information sharing among role players, e.g., accountable institutions (AIs), law enforcement, and Financial Intelligence Units (FIUs), further impede efforts to disrupt economic crime.

International measures to address economic crime have been introduced through various instruments such as the *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (the *Vienna Convention*) in 1988; the *United Nations Convention Against Transnational Organised Crime* (the *Palermo Convention*) in 2000; and the *United Nations Convention Against Corruption* (*UNCAC*) in 2003. These initiatives promote the confiscation of the proceeds of crime, the criminalisation of money laundering (ML), the implementation of reporting duties and compliance procedures, and the establishment of the FATF with its global standards, namely the FATF Recommendations to Combat ML/TF and Proliferation Financing (PF).[12]

South Africa's Anti-Money Laundering and Terrorism Financing (AML/CFT) framework dates from the 1990s and is embodied in several key pieces of legislation: the *Drugs and Drugs Trafficking Act* 140 of 1992 (the first legislation addressing ML); the *Proceeds of Crime Act* 76 of 1996 (which criminalises any proceeds from criminal activities); the *Prevention of Organised Crime Act* 121 of 1998 (*POCA*); the *Financial Intelligence Centre Act* 38 of 2001 (*FICA*) (which established the Financial Intelligence Centre (FIC) and reporting duties);[13] and the *Protection of Constitutional Democracy Against Terrorist and Related Activities Act* 33 of 2004

8 Basel Institute on Governance 2018 https://baselgovernance.org/sites/default/files/2019-02/basel_aml_index_10_09_2018.pdf.

9 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

10 Kruger *Organised Crime and Proceeds of Crime Law* 3-4; Management Solutions 2023 https://www.managementsolutions.com/sites/default/files/minisite/static/7805cb71-d48b-407e-9c40-9353639337c7/fincrime/pdf/financial-crime-en.pdf.

11 Europol 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

12 De Koker *et al* 2025 *Money Laundering* 6-7.

13 De Koker *et al* 2025 *Money Laundering* 22.

(*POCDATARA*) (which criminalises terrorism and related offences and provides measures to combat TF). However, the Anti-Money Laundering, Counter-Terrorism Financing, and Proliferation Financing (AML/CFT/PF) regime has not yielded the desired results nationally or internationally, as economic crimes continue to flourish despite a costly compliance system. It is estimated that €4 trillion is laundered every year, of which around 1-2 per cent is successfully confiscated under current compliance practices, at costs of €100-150 billion annually for banks on compliance staff and technology.[14] Alternative measures and approaches are urgently required.[15]

The *Prevention and Combating of Corrupt Activities Act* 12 of 2004 (*PRECCA*), enacted in compliance with South Africa's status as a signatory to *UNCAC*, establishes a broad reporting duty in section 34(1), encompassing not only the different Chapter 2 iterations of corruption but also offences such as theft, fraud, extortion, forgery, or the uttering of a forged document involving amounts of R100,000 or more.[16]

Section 29 of *FICA* requires that individuals conducting business or managing a business, or employed by a business, report suspicious transactions potentially linked to ML/TF or related activities to the FIC.[17] Similarly, section 12 of *POCDATARA* imposes a duty to report suspicions of committing or the intention to commit terrorism-related offences to the South African Police Services (SAPS).[18]

These reporting duties, as well as the due diligence and record-keeping requirements mandated by the AML/CTF/PF framework, are rooted in one essential concept: access to and the sharing of information.[19] The private sector, particularly financial institutions (FIs), have access to a wealth of information and can therefore play a crucial role in disrupting economic crime.[20] Financial institutions represent the first line of defence against

14 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

15 UK Finance 2018 https://www.parliament.uk/globalassets/documents/commons-committees/treasury/Written_Evidence/ecr0064.pdf; De Koker *et al* 2025 *Money Laundering* 7; Deloitte 2024 https://www.deloitte.com/content/dam/assets-zone2/uk/en/docs/services/financial-advisory/2024/fa-article75-thought-leadership-final.pdf.

16 *Prevention and Combating of Corrupt Activities Act* 12 of 2004 (*PRECCA*) preamble, section 34.

17 Section 29 of the *Financial Intelligence Centre Act* 38 of 2001 (*FICA*).

18 Section 12 of the *Protection of Constitutional Democracy Against Terrorist and Related Activities Act* 33 of 2004 (*POCDATARA*).

19 De Koker *et al* 2025 *Money Laundering* 237.

20 Home Office and HM Treasury 2016 https://assets.publishing.service.gov.uk/media/5a74e52440f0b65c0e8455bd/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf; FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

economic crime;[21] however, their capabilities are limited, as they often have only a partial view of transaction flows.[22] Customer confidentiality obligations and privacy provisions further prevent FIs from sharing information.

The concept of public-private information sharing[23] has recently been advanced through mechanisms such as the South African Money-Laundering Integrated Taskforce (SAMLIT) under the auspices of the broader AML/CTF/PF framework.[24] Formalised information sharing between private sector entities is, however, necessary to bolster the disruption of economic crime. Fifteen private-to-private (P2P) frameworks have been identified internationally.[25] Establishing a local P2P framework could be the next frontier in strengthening the country's capacity to disrupt economic crime. A first step was taken by the Legislature through the 2022 enactment of section 41A(3) of *FICA*.[26] This was followed by the publication of its envisioned embodiment in the *Draft Amendment*[27] to the *Money Laundering and Terrorist Financing Control Regulations*[28] (the *Draft Amendments*), in September 2023. This paper explores the concept and necessity of P2P information sharing and conducts an individualising comparative analysis of selected international P2P frameworks to identify best practices for the implementation of a P2P framework for South Africa. This analysis encompasses the US model of information sharing in terms of section 314(b) of the *PATRIOT Act*,[29] Singapore's Collaborative Sharing of

---

21 Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023; FATF 2025 https://www.fatf-gafi.org/en/publications/Fatfgeneral/pscf-march-2025.html.

22 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

23 Public-private information sharing encompasses diverse models of cooperation and can range from informal initiatives to mandated arrangements between public and private sector entities.

24 FIC date unknown https://www.fic.gov.za/about/; Wannenwetsch 2023 https://baselgovernance.org/news/partnering-against-money-laundering-and-corruption-south-africa-and-subregion.

25 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

26 The *General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act* 22 of 2022 amended *FICA* to bring s 41A(3) into force.

27 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf (the *Draft Amendments*).

28 GN R1595 in GG 24176 of 20 December 2002 (*Money Laundering and Terrorist Financing Control Regulations*).

29 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* 56 of 2001 (the *USA PATRIOT Act*). The purpose of this Act is to discourage and punish terrorist acts in the USA and around the world and strengthen law enforcement investigation tools.

ML/TF Information and Cases (COSMIC), Transaction Monitoring Netherlands (TMNL), and Estonia's AML Bridge.

2 Research approach and methodology

An individualising comparative analysis is a research methodology utilised for the systematic analysis of differences and similarities across a small number of cases.[30] It comprises four key features: a frame of reference (i.e., the question, problem, idea, or theory underpinning the research), grounds for comparison, similarities and differences, and the thesis.[31] The analysis relies on secondary data from publicly available sources. The central research question is: How can the South African P2P framework be improved to enhance the disruption of economic crime?

The aforementioned P2Ps were identified from the FATF's paper on Data Protection, Technology and Private Sector Information Sharing[32] as successful examples that align with FATF's requirements, which South Africa must also adhere to. The paper identifies similarities and differences between the proposed SA P2P framework – embodied in section 41A(3) of *FICA* and the *Draft Amendments* – and the comparator frameworks, focussing on functionalities central to P2P frameworks. These include the protection of personal information, the maintenance of confidentiality and integrity, the methods and types of information that may be shared, and the public sector's role. The thesis, the final key feature, addresses whether the similarities outweigh the differences, or vice versa, or whether they hold equal weight.[33] This is discussed in the conclusion of the paper.

The paper refers to economic crime, acknowledging that its various manifestations – ML/TF/PF, fraud, cybercrime, and corruption – entail illicit financial flows and can all benefit from P2P information sharing. Addressing ML is interlinked with the combating of predicate crimes thereto. For instance, corruption is a common predicate offence to ML, as countries with high levels of corruption face a greater risk of ML.[34] The sharing of information is, therefore, not only relevant to combating ML but also to its

30 Onwuegbuzie and Weinbaum 2017 *The Qualitative Report* 362-363; Pickvance 2001 *Journal of Housing and the Built Environment* 16.

31 Walk 1998 https://cbs.umn.edu/sites/cbs.umn.edu/files/migrated-files/downloads/Compcontrastharvard.pdf.

32 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

33 Rose 2019 https://www.edb.gov.hk/attachment/en/curriculum-development/kla/eng-edu/professional-development-programmes/1920/LiE_Comparative_Analysis_20200337.pdf.

34 Basel Institute on Governance 2025 https://baselgovernance.org/basel-aml-index/methodology/indicators.

predicate crimes.[35] A comparative analysis using secondary data was conducted of key aspects of the proposed P2P framework against selected international P2Ps, from the USA, Singapore, the Netherlands and Estonia.

3 The need for, advantages of, and definition of P2Ps

Maxwell defines a P2P as "a specific institutionalised form of collaboration [between private sector entities], with a governance framework and some level of permanence to its existence".[36] P2Ps involve collaboration, innovation, data interoperability and privacy-enhancing technologies.[37] They require the horizontal integration of information and should not treat ML and fraud as separate issues but rather address the entire spectrum of economic crimes.[38]

FATF argues that effective information sharing is one of the cornerstones of a well-functioning AML/CFT framework.[39] Information and intelligence allow FIs to perform trend analyses, focus on suspects or geographical vulnerabilities and patterns of behaviour that can be detrimental to the monitoring of transaction flows, manage risk exposure, and provide valuable input to law enforcement.[40]

However, FIs individually are limited to the information available within their institution or from publicly available sources such as social media, media reports or public registers.[41] They often lack the broader context of specific transactions, making it difficult to identify suspicious activities, as criminals frequently employ sophisticated structures and transaction flows across numerous FIs,[42] corporate entities and jurisdictions to facilitate their crimes or launder the proceeds of crime in the case of ML/TF.[43] Furthermore, P2Ps

35 FATF 2023 https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

36 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

37 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

38 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

39 FATF 2017 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf; FATF 2024 https://www.fatf-gafi.org/en/the-fatf/mandate-of-the-fatf.html.

40 FATF 2017 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.

41 Publicly available sources are information that is legally accessible by the general public; for example a city council meeting published in the Sunday Times.

42 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

43 De Koker *et al* 2025 *Money Laundering* 4-5.

enable FIs to share information and perform collaborative analyses to mitigate, assess, and understand their economic crime risks.[44] With information from another FI, an FI can pinpoint suspicious transactions that may initially have appeared innocuous.[45]

FATF Recommendation 20 requires FIs and other private sector entities to identify and report suspicions of ML/TF to their respective national FIUs.[46] By expanding the understanding of criminal activity beyond their own data limitations and avoiding siloed perspectives, P2Ps not only assist FIs in identifying and reporting suspicious activities but also reduce false positives. This, in turn, enhances the effectiveness and efficiency of the AML/CTF/PF framework, which has faced increased criticism due to costly and protracted AML screening and compliance requirements for customer onboarding. Legitimate customers have experienced negative impacts from strict transaction monitoring that blocks or delays legitimate transactions, leading to unintended consequences such as financial exclusion or debanking.[47] AML systems are prone to human error and can generate high volumes of false positives due to the manual processes for drafting Suspicious Activity Reports (SARs),[48] incomplete and outdated customer data, and stringent AML compliance systems.[49]

A 2017 FATF Guidance on private sector information sharing states that, although no specific FATF Recommendation refers to P2P, Recommendations 18 (concerning internal controls and foreign branches and subsidiaries), 20 (concerning the reporting of suspicious transactions), and 21 (concerning tipping-off and confidentiality) correlate with information sharing.[50]

P2Ps offer various benefits:

---

44 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

45 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

46 FATF 2025 https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf.coredownload.inline.pdf.

47 De Koker and Casanovas "'De-risking', De-banking and Denials of Bank Services" 46; La Trobe University 2025 https://www.latrobe.edu.au/news/announcements/2025/lowering-global-barriers-to-financial-inclusion; Onwuegbuzie and Weinbaum 2017 *The Qualitative Report* 362-363.

48 A Suspicious Activity Report (SAR) is a report submitted in terms of section 29(1)(a), (c) or 29(2) of FICA relating to suspicious or unusual activity, money laundering (ML), proceeds of unlawful activities or contraventions of s 26B.

49 Alessa 2024 https://alessa.com/blog/how-to-reduce-aml-false-positives/; Yuklea 2025 https://www.feedzai.com/blog/aml-roi/.

50 FATF 2017 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.

- They enhance customer identification, as entities can verify a client's risk rating against other entities to determine whether the client has previously raised red flags.[51]

- Transaction monitoring is improved, as well as sanctions or other screenings, assisting in the quicker and more efficient identification of suspicious activity and screening of customers and counterparties in transactions against the United Nations' and domestic sanctions lists.[52]

- As criminals can be onboarded by multiple institutions, P2Ps help FIs continuously update their customer information.[53]

- FIs are assisted in identifying beneficial owners across institutions, specifically regarding shell companies.[54]

- More accurate and timely identification of crime typologies is enabled, allowing for better safeguards to prevent the same crime from recurring.[55]

- They help broaden the scope of data that can be analysed, as such analysis does not need to be conducted in silos. In this way, criminals are prevented from exploiting multiple FIs and reducing the risk of illicit funds being displaced in the financial system. Entities can assist one another in recovering such funds and assets.[56]

- They further assist entities in the early identification of risks, which facilitates the timely implementation of preventative measures and consequence management processes to mitigate potential damages. P2Ps allow entities to identify risks that may not have matured yet or

---

51 FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

52 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

53 FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

54 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

55 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

56 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf; Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf; IMC 2024 https://www.mas.gov.sg/-/media/mas-media-library/news/media-releases/2024/imc-report.pdf

that they might not have been able to detect independently. This reduces the duplication of risk identification and the concomitant deployment of resources by multiple entities.[57] This approach aligns with fraud risk management strategies, where the prevention and detection of economic crime are central, potentially including continuous control monitoring and proactive data analysis.[58]

- P2Ps facilitate the optimisation of real-time or near real-time information, aiding in the swift disruption of economic crime. They allow for the collation of data, expertise and resources from multiple entities, which can support large-scale data analytics and machine-learning capabilities.[59]

- P2Ps enable more informed decisions regarding client de-risking, as the sharing of intelligence among FIs assists in eliminating uncertainty about whether to terminate a client's relationship.[60]

4 Key considerations

For a P2P to function effectively, three key aspects must be present: "a shared strategic vision between public and private sector stakeholders … a clear enabling legislative and regulatory environment … [and] a framework of good governance, data ethics and accountability".[61]

Clearly defining the roles of each sector and their ability to identify and respond to economic crime threats is essential for establishing a shared strategic vision. Clarity should also be provided regarding the nature and extent of the information to be shared and the connectivity obligations that need to be met. The latter is particularly important to ensure the protection of personal information by limiting the information shared to a "need to have" basis.[62]

---

57 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

58 Harris "Fraud Risk Management".

59 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf; Goldbarsht "Private to Private".

60 Goldbarsht "Private to Private".

61 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf; Goldbarsht "Private to Private".

62 Pedersen *Investigator's Guide to Open-Source Intelligence* 22.

Two factors contribute to a successful legislative and regulatory environment.[63] First, a clear policy commitment should enable information sharing within legal boundaries, taking privacy and competition laws into account and providing protection against defamation liability. Second, regulatory guidance should confirm that information sharing is both permitted and encouraged.[64] Data protection and the protection of the right to privacy (DPP) are crucial to the functioning of a P2P,[65] although the specific approach and extent may differ between jurisdictions.

DPP generally include the ability to control who may access or use a person's or entity's personal information, as enshrined in data protection laws that require transparency regarding how data are collected, used and shared, while safeguarding against intrusion. They typically limit disclosure to institutions by means of informed consent or other legal grounds, while granting individuals the right to access, correct or delete their data and to seek redress for privacy violations, subject to exceptions such as national security and law enforcement. DPP frameworks often include exceptions, exemptions, restrictions or limitations to privacy rights, particularly regarding ML, fraud or terrorism. However, they also help mitigate legal risks, especially across jurisdictions, and enhance public trust. Despite these exceptions, stakeholders often find it challenging to apply core data protection principles when developing and implementing P2P. Privacy Enhancing Technology is therefore employed to ensure that the necessary privacy measures are in place to maintain the confidentiality of personal information while supporting information sharing and protecting personal data and privacy.[66]

FATF's 2022 *Data Protection, Technology and Private Sector Information Sharing Report* highlights key aspects from various jurisdictions' DPP frameworks, including the type of personal information that may be shared, the legal basis for sharing, its purpose and its use. Such sharing should be reasonable, proportionate and necessary. For instance, data should not be retained longer than necessary, should not include excessive information, and should align with the purpose for which they are processed. Personal data must be collected and maintained accurately, reliably, consistently, and

63 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

64 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf; Goldbarsht "Private to Private".

65 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

66 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

completely, with processing conducted fairly and lawfully. The FATF (2022) report further states that the integrity of personal information is preserved when the information is reliable, accurate, consistent, complete, and in context. Data subjects should be informed about who will process their data, the purpose of the processing, and the scope of the processing. In the event of a data breach, both the data subjects and the authorities must be notified. The use and processing of data should be subject to oversight by one or more independent bodies capable of effective supervision, either individually or cumulatively. Additionally, appropriate measures should be in place to allow individuals to complain or seek redress regarding any alleged improper processing of their personal information or to access or correct their personal information. Some jurisdictions require an impact assessment to help institutions minimise the risks related to the collection, processing, distribution and use of personal data.[67]

A concern arises regarding some P2Ps established under AML/CFT legislation which may not have the authority or scope to address issues such as fraud attacks and scam transactions (FAST).[68] Fraud and scams have a close relationship with ML/TF, being considered predicate offences in some jurisdictions only.[69] Accordingly, cooperation on such cases falls under a different legal regime than standard AML P2Ps. When a country treats FAST as a predicate offence and has AML P2P laws in place, entities can use these laws to share information on FAST-related threats. Additionally, entities may rely on alternative legal gateways for sharing FAST-related risk information, providing multiple legal avenues for P2P information sharing in response to FAST threats.[70]

Certain policy issues may arise when establishing a P2P. Although P2Ps occur between private sector entities, the public sector can play a role in their successful establishment, according to FATF. P2Ps lacking government support may struggle to gain the support of peers or receive feedback from DPP authorities or suffer from poor coordination and communication. Moreover, the level of public sector involvement varies depending on the objectives and functioning of the P2P and the willingness of public authorities to provide assistance. The sharing of information between private sector entities may not necessarily align with a country's AML/CFT/CPF priorities and objectives, especially when the initiative is not

67 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf; Malahleka 2024 *PELJ* 24.

68 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

69 De Koker *et al* 2025 *Money Laundering* 46.

70 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

led by a prominent government agency. This misalignment could be detrimental to information sharing, as engagement between these two sectors is crucial for clarity, improving information sharing, and avoiding conflicts arising from a lack of mutual understanding regarding the public interest in protecting both the public from crime and whilst safeguarding personal data and privacy.[71]

5 P2Ps in South Africa

Although a formal P2P framework is currently being established, some unregulated sectoral P2Ps are in existence, four of which are discussed below.

5.1 South African Fraud Prevention Services (SAFPS)

The SAFPS is a non-profit organisation (NPO) established in 2001, dedicated to: "improv[ing] vigilance with regards to fraud, financial crime and identity theft by educating businesses and consumers … and assisting them to protect themselves".[72] Its vision acknowledges that becoming a front runner against economic crime depends on harnessing the "power of collaboration" across the public and private sectors, and consumers.[73] The SAFPS' board of directors consists of 12 members representing private sector entities.[74] Its 104 members include private sector subscribing members from the major banks, asset finance, cash-in-transit service providers, investment, clothing retail, telecoms, furniture retail, fintech, insurance, microfinance, and reseller companies. These members collaborate by sharing information on fraud detection and prevention techniques, fraudulent incident data, and financial crime solutions. The National Lotteries Commission is a public sector subscribing member. Affiliate members include the Australian Financial Crime Exchange, Cifas, the Insurance Crime Bureau (ICB), South African Banking Risk Information Centre (SABRIC), Transunion, Experian, and Xpert Decision Systems. Public sector affiliate members include the FIC, the Department of Home Affairs, the South African Revenue Service, the Financial Sector Conduct Authority, and the South African Reserve Bank (SARB).[75]

---

71 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

72 SAFPS 2025 https://www.safps.org.za/Home/About; SAFPS 2025 https://www.safps.org.za/#:~:text=MAKING%20A%20DIFFERENCE,as%20possible%20expansion%20into%20Africa.

73 SAFPS 2025 https://www.safps.org.za/Home/About.

74 SAFPS 2025 https://www.safps.org.za/#:~:text=MAKING%20A%20DIFFERENCE,as%20possible%20expansion%20into%20Africa.

75 SAFPS 2025 https://www.safps.org.za/Home/Article_SAFPS_Annual_Report_2024; SAFPS 2025 https://www.safps.org.za/Home/OurPartners.

The SAFPS operates a fraud database that helps its members identify and prevent fraudulent activities while safeguarding consumers from schemes such as identity fraud. The organisation also provides protective registration services to individuals who have fallen victim to identity fraud, Identification Document (ID) or passport theft, or any form of identity compromise, offering protection against further losses.[76]

At its core the SAFPS supports its members by fostering a collaborative fraud-fighting community through data sharing and trend analysis. A secure collaboration forum, launched in 2024, allows members to share real-time information, including a perpetrator's name and surname, passport or ID number, birth date, email address, home address, telephone numbers, employer details, and bank account details.[77] [78]

5.2 Communications Risk Information Centre (COMRiC)

COMRiC is an NPO established in 2020 by role players in the SA telecommunications industry to maintain, support and develop practical commercial-crime and risk-combating capabilities. [79] COMRiC enters into beneficial collaboration agreements to create a "trusted sector-led platform that could anticipate and disrupt criminal networks targeting South Africa's digital infrastructure".[80]

COMRiC is governed by a board of directors consisting of the founding members of the organisation, chaired by an independent non-executive. The directors hail from the four largest telecommunications companies and a pan-African digital infrastructure company.[81] COMRiC also has public-private information sharing systems in place through partnerships with the Directorate for Priority Crime Investigation of SAPS and Interpol. COMRiC works alongside financial service providers, telecommunication alliances, and the government to safeguard telecommunication infrastructure.[82] They enable these cross-sector partnerships by acting as an independent facilitator, advocacy voice, and knowledge-sharing platform that aligns public sector accountability and private sector agility.[83] The organisation

---

76 SAFPS 2025 https://www.safps.org.za/Home/About.
77 SAFPS "South African Fraud Prevention Services".
78 SAFPS 2025 https://www.safps.org.za/Home/Article_SAFPS_Annual_Report_2024.
79 COMRiC 2023 https://comric.co.za/wp-content/uploads/2023/06/COMRiC-Website-Privacy-Notice-130623.pdf.
80 COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf.
81 COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf.
82 COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf.
83 COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf.

further assists in regulatory coordination with regard to cyber security by serving as a central hub for collaboration. It shares threat intelligence, coordinates responses to cyber incidents, develops best practices to improve sector-wide cyber resilience, and provides submissions on relevant legislation.[84] A key aspect identified in the COMRiC 2025 Telecommunications Sector Report is the need for cross-sector collaboration and intelligence sharing[85] to mitigate emerging and current risks and reinforce the strategic role of the telecommunications sector within the country's economic ecosystem.[86]

5.3 SABRIC

SABRIC is an NPO established in 2002 by South Africa's banking industry to curb organised crime through effective crime risk information sharing, fraud prevention, and mitigation strategies.[87] SABRIC adopts a cooperative strategy that strengthens collaboration among financial institutions, law enforcement, government entities and other key stakeholders. This contributes to establishing a collective defence against economic crime and fosters a stronger, more secure financial system.[88]

SABRIC has 16 private sector members, which include banks, a financial technology company, and a money transfer company. In 2024 SABRIC signed Memorandums of Understanding with the Department of Justice and Constitutional Development, Eskom, the State Security Agency, and the South African Development Community Banking Association. Real-time information sharing contributed to resolving 2,169 ATM incidents, according to its 2024 report. Additionally it assisted in 35 arrests related to kidnapping cases and facilitated the drafting and implementation of the Kidnapping for Ransom Information Sharing Framework.[89]

5.4 ICB

The ICB is an NPO launched in 2008 at the request of the South African Insurance Association (SAIA) to holistically enable short-term insurance companies to combat fraud and crime more effectively, including vehicle

84 COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf.

85 Mvelase 2025 https://www.businesslive.co.za/bd/opinion/2025-07-31-thokozani-mvelase-cybercrime-is-a-state-of-emergency-in-sa/.

86 COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf.

87 DoJCD 2016 https://www.justice.gov.za/m_speeches/2016/20161027-dm-SABRIC.html; SABRIC 2025 https://www.sabric.co.za/about-sabric/.

88 SABRIC 2025 https://www.sabric.co.za/.

89 SABRIC 2025 https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf.

theft, medical and life insurance fraud, and homeowners' claims.[90] The ICB strives to provide intelligence and promote collaboration to prevent and detect fraud and crime, obtain convictions and recover stolen assets.[91]

The ICB is a membership-based organisation supported by industry partners and law enforcement agencies providing its members with access to fraud prevention and detection capabilities, insurance fraud training, data analytics and public awareness campaigns.[92] Its 26 members include banks and short-term insurance companies, while associate members comprise companies that render security, automotive, electronic, data and artificial intelligence services.

The ICB is governed by a board of directors consisting of an independent chairman and representatives from ICB members and SAIA.[93] A central Intelligence Hub has been established for members to gather resources and information and foster opportunities for collaboration.[94] Real-time information sharing between law enforcement and financial institutions is facilitated through a secure digital platform.[95]

5.5 The Draft Amendments

In September 2023 the National Treasury called for public comments to be submitted a month later[96] on the *Draft Amendments* to the *ML and TF Control Regulations* of 2002 (the *ML Regulations*).[97] The aim was to set out requirements for the sharing of information between AIs.[98] This followed the enactment of section 41A(3) of *FICA*, through section 26 of the 2022 *General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act*, which was enacted to assist the country's efforts in exiting the FATF's greylist.[99] Section 41A(3) allows the Minister of Finance (the Minister) to

---

90 ICB 2025 https://www.saicb.co.za/pages/company-profile; ICB 2025 https://www.saicb.co.za/pages/company-history; ICB 2025 https://www.saicb.co.za/pages/membership.

91 ICB 2025 https://www.saicb.co.za/pages/company-profile.

92 ICB 2025 https://www.saicb.co.za/pages/membership.

93 ICB 2025 https://www.saicb.co.za/uploads/files/Insurance-Crime-Bureau-2024-Annual-Report.pdf.

94 ICB 2025 https://www.saicb.co.za/uploads/files/Insurance-Crime-Bureau-2024-Annual-Report.pdf.

95 ICB 2025 https://www.saicb.co.za/uploads/files/Insurance-Crime-Bureau-2024-Annual-Report.pdf.

96 PMG 2023 https://pmg.org.za/call-for-comment/1362/.

97 Published in GN R1595 in GG 24176 of 20 December 2002.

98 Moonstone Information Refinery 2023 https://www.moonstone.co.za/draft-amendments-on-information-sharing-between-accountable-institutions-published/.

99 PMG 2022 https://pmg.org.za/committee-meeting/35924/; De Koker *et al* 2025 *Money Laundering* 237.

> prescribe requirements for the protection of personal information to facilitate the sharing of information between accountable institutions when the sharing of information is necessary for the purposes of carrying out the provisions of section 29 [suspicious and unusual transactions].

Section 41A(3) formally introduces P2P into the SA AML regime, applicable only to AIs and for the purposes of section 29 reporting duties,[100] whilst allowing for the protection of personal information.[101] Twenty AIs are identified in section 1, read with Schedule 1, of *FICA*,[102] as revised in December 2022. These institutions range from legal practitioners, estate agents and banks to life insurance businesses, businesses dealing in high-value goods, and crypto-assets service providers – essentially any institution vulnerable to ML/TF/PF abuse.[103] Several compliance and reporting obligations are imposed by *FICA* on various persons and entities, specifically requiring AIs to register with the FIC and provide information that is kept in a register.[104]

The *Draft Amendments* will introduce a new regulation, Regulation 27E (discussed below), to the *ML Regulations*, as well as sub-regulation 7(A) to Regulation 29. This will render any person or institution that fails to "share the information of a client" or notify the FIC accordingly as non-compliant and subject to administrative sanction.[105]

The Explanatory Memorandum to the *Draft Amendments* (the Explanatory Memorandum) confirms that "the ability to share information is critical to identifying, reporting, and preventing financial crime".[106] It acknowledges that, without information sharing, it is "difficult" for AIs to recognise and report suspicious activity due to their limited view of the broader context – a weakness that is exploited by criminals and terrorist organisations to move illicit funds within the financial system. This impedes the legislative mandate and key capability of the FIC to "follow the money", i.e., to "generate a view of how funds move from one person or institution to another", which flows

---

100 A section 29 report must be made when any person involved in a business becomes aware or suspects that they are going to receive funds originating from unlawful activities, or property linked to terrorism financing (TF), or that they are being used for ML purposes or are used to assist in an offence relating to ML/TF. A section 29 report must be filed with the FIC.

101 De Koker *et al* 2025 *Money Laundering* 237.

102 Schedule 1 of *FICA*.

103 FIC 2022 https://www.fic.gov.za/wp-content/uploads/2023/09/2022.12-CG-FIC-Act-reference-guide.pdf.

104 Section 43(B)(1) and (3) of *FICA*.

105 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

106 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

are mainly generated from information contained in reports AIs make to the FIC.[107]

Five aspects, discussed below, are key to the *Draft Amendments:* information sharing must comply with *FICA* and the *Protection of Personal Information Act* 4 of 2013 (*POPIA*); the integrity and confidentiality of personal information must be ensured; information may be shared only in accordance with a written agreement; AIs must notify the FIC and keep record of information shared; and the impact of shared information on de-risking and defensive reporting must be considered.[108]

5.5.1 Compliance with relevant legislation

Section 27E(1) of the *Draft Amendments* stipulates that:

> for the purposes of carrying out the provisions of section 29 as contemplated in section 41A(3) of the Act, an accountable institution must ensure the integrity and confidentiality of the personal information of the client … to prevent—
> *(a)* alteration or loss of, damage to or unauthorised destruction of the information; and
> *(b)* unlawful access to or further processing of the information, other than in accordance with the Act and [POPIA].[109]

Section 27E(3) states that an:

> accountable institution must comply with the requirements relating to disclosure contained in section 29 of the Act when sharing information relating to a client as per section 41A(3).[110]

The Explanatory Memorandum emphasises that the "utmost circumspection must be maintained" when sharing the content of reports about suspicious or unusual transactions or activities, or the fact that such reports were made, and that information sharing must comply with sections 29(3) and (4) of *FICA*.[111] The phrase "suspicious or unusual transactions or activities" is understood to encompass SARs, suspicious or unusual transaction reports

---

107 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

108 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

109 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

110 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

111 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

(STRs), terrorist financing activity reports, and terrorist financing transaction reports.[112]

Section 29(3) prohibits the person who made the report from disclosing any information regarding the contents of suspicious and unusual transaction reports. Section 29(4) prohibits anyone who knows or suspects that a report has been made from disclosing such suspicions or any information regarding the suspected contents of the report. However, disclosures are permitted in four instances: when made for the purposes of carrying out specific powers and duties in terms of any legislation, for carrying out the provisions of *FICA*, for the purposes of legal proceedings, or in terms of a court order.[113]

The Explanatory Memorandum emphasises that the principles related to the protection of personal information,[114] as per *POPIA*, must be followed when sharing customers' personal information. Compliance is not optional, and a claim of adherence to the reporting obligations under *FICA* cannot be used as a defence.[115]

POPIA regulates

> the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy [as per section 14 of the Constitution of the Republic of South Africa, 1996] subject to justifiable limitations that are aimed at protecting other rights and important interests.[116]

Section 6 provides for exclusions. Notably, *POPIA* does not apply to the processing of personal information when such information:

---

112 See the definitions of these concepts in the 2017 *ML/TF Control Regulations* (GN R1062 in GG 41154 of 29 September 2017).

113 Section 29(3) and (4) of the *Draft Amendments*.

114 Section 1 of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*) defines personal information as "information relating to an identifiable, living, natural person, and an identifiable, existing juristic person, including, *inter alia*–

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person."

115 National Treasury 2023 https://www.treasury.gov.za/Legislation/ Regulations/ Draft%20Regulations%20-%20Sharing%20of%20information %20between%20accountable%20institutions.pdf.

116 The preamble of *POPIA*.

- "has been de-identified to the extent that it cannot be re-identified again"[117] or

- when processed

> by or on behalf of a public body—
> (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or
> (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders … to the extent that adequate safeguards have been established in legislation for the protection of such personal information.[118]

Chapter 3 of *POPIA* sets out specific conditions for the lawful processing of personal information, including accountability, processing limitations, purpose specification, information quality, openness, security safeguards, and data subject participation.[119] Part B of Condition 8 (data subject participation) – sections 26 to 33 – addresses the processing of special personal information.[120] Section 26 defines special personal information, which may not be shared except under the exceptions outlined in section 27.[121] Sections 28 to 33 provide additional exemptions to the prohibitions in section 26 regarding each specific type of special personal information.[122]

Section 27(2) mandates the Information Regulator (IR) to grant exemptions to the right to privacy.[123] The IR is an independent body established under section 39 of *POPIA* to monitor and enforce compliance by private and public bodies with *POPIA* and the *Promotion of Access to Information Act* 2 of 2000.[124] Section 26 defines "special personal information" and states that a responsible party may not, subject to section 27, process personal information concerning:

> (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
> (b) the criminal behaviour of a data subject to the extent that such information relates to-
> (i) the alleged commission by a data subject of any offence; or

117 Section 6(1)(b) of *POPIA*.
118 Section 6(1)(c) of *POPIA.*
119 Chapter 3 of *POPIA*.
120 Part B Condition 8 of *POPIA*.
121 Section 26 of *POPIA*.
122 Sections 28-33 of *POPIA*.
123 IR 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/Guidance-Note-Processing-Special-PersonalInformation-20210628-004.pdf; SAPS 2021 https://www.saps.gov.za/resource_centre/paia/public_manual_popia_2021.pdf.
124 IR 2025 https://inforegulator.org.za/about/.

> (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.[125]

Section 33(1) states:

> the prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in section 26, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.[126]

A "responsible party" is defined as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".[127]

Chapter 4 provides exemptions for the processing of personal information. Processing is not considered a breach if the IR grants an exemption under section 37 or if the processing is compliant with section 36. Section 37(1) grants the IR the discretion to allow a responsible party to process personal information, "even if that processing is in breach of a condition for the processing of such information", if, in the circumstances of the case:

> (a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or
> (b) the processing involves a clear benefit to … a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.[128]

"Public interest" is defined in section 37(2) and includes the interests of national security, the prevention, detection and prosecution of offences, the significant economic and financial interests of a public body, or promoting compliance with legal provisions related to the interests described in paragraphs *(b)* and *(c)*.[129]

Section 38(1) provides for exemptions for the processing of personal information for the purpose of discharging a relevant function. Exemption from sections 11(3) and (4) (concerning objections from the data subject), 12 (concerning collection directly from the data subject), 15 (concerning further processing compatible with the purpose of collection), and 18 (concerning notification to the data subject when collecting personal information) is provided "in any case to the extent to which the application of those provisions to the personal information would be likely to prejudice the proper discharge of that function".[130]

---

125 Sections 1 and 26 of *POPIA*.
126 Section 33(1) of *POPIA*.
127 Section 1 of *POPIA*.
128 Section 37(1) of *POPIA*.
129 Section 37(2) of *POPIA*.
130 Section 38(1) of *POPIA*.

Subsection 38(2) defines "relevant function" as:

> any function—
> (a) of a public body; or
> (b) conferred on any person in terms of the law,
> which is performed with the view to protecting members of the public against—
> (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or
> (ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity.[131]

Privacy laws in certain jurisdictions such as the European Union's (EU) General Data Protection Regulation (GDPR) permit information sharing in respect of fraud and ML. Recital 47 of the GDPR states that personal information may be shared to prevent fraud, provided this is in the legitimate interests of the data controller.[132] *POPIA* provides for exemptions that facilitate the lawful processing of personal information. However, it remains unclear whether P2P, or the sharing of information between AIs for purposes of section 29 reporting under *FICA* as envisioned by the *Draft Amendments*, will qualify for exemption.[133] Clarity in this regard, either via specific legislation or the discretion provided to the IR in section 37 of *POPIA*, is required, as the provisions of *POPIA* may severely limit information sharing.

5.5.2 Ensuring the integrity and confidentiality of personal information

In addition to the requirements for securing the integrity and confidentiality of personal information in section 27E(1) (see above), subsection 27E(2) states that an AI must:

> (a) identify all reasonably foreseeable internal and external risks related to the transmission of the information;
> (b) establish and maintain appropriate safeguards against the risks identified;
> (c) regularly verify the effective implementation of the safeguards; and

131 Section 38(2) of *POPIA*.

132 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

133 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

(d) ensure continual updates of the safeguards.[134]

A continuous process of risk assessment, development and implementation of measures to ensure the integrity and confidentiality of the information to be shared is required. However, the requirement to identify "all" reasonably foreseeable internal and external risks may be excessive.

The Explanatory Memorandum warns that the sharing of customer data presents the risk of exploitation or unauthorised access; hence the importance of protection and security when sharing customer information between AIs to maintain public trust and prevent harm to the individuals involved.[135] The Memorandum suggests that participating AIs develop a platform for engaging and exchanging information, considering technological advancements such as encryption and data pseudonymisation. *FICA* overrides the confidentiality and secrecy obligations of South African law, as per the provisions of Chapter 3 of *FICA*, except in respect of legal professional privilege.[136]

5.5.3 Contractual approval for information sharing

Section 27E(4) stipulates that information sharing "may only occur in accordance with a written agreement between the AIs that regulates the exchange of information".[137] The Explanatory Memorandum emphasises that AIs must agree on the scope of the customer information to be shared, especially when in the process of forming a suspicion.[138] They should also provide "reasonable assurance" regarding the reliability and accuracy of the shared customer information to enhance effectiveness and prevent the reporting of "false positives" or the concealment of reportable suspicions.[139] The term "reasonable assurance" is, however, not defined in *FICA* or the Explanatory Memorandum.[140] Any written agreement for information sharing does not exempt AIs from the duty to submit section 29 reports.[141]

---

134 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

135 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

136 De Koker *et al* 2025 *Money Laundering* 210.

137 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

138 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

139 Moonstone Information Refinery 2023 https://www.moonstone.co.za/draft-amendments-on-information-sharing-between-accountable-institutions-published/.

140 Reasonable assurance is defined as "a high but not absolute level of assurance".

141 Section 52 of *FICA*.

5.5.4 Notification to the FIC and record keeping

Sections 27E(5) and (6) state that, within five days after the information is shared, the AI must notify the FIC of the name of the receiving AI, the identifying particulars of the client, and the date of sharing. AIs are not required to obtain permission from the FIC to share information.[142]

Sections 27E(7) and (8) mandate that, when a receiving AI has reasonable grounds to believe that a client's personal information has been accessed or obtained by any unauthorised person, the receiving AI must notify both the FIC and the AI that shared the information as soon as is reasonably possible, but no later than five days after discovering the compromise.

Notification to the FIC is justified in the Explanatory Memorandum, firstly, by "the sensitivity of the information to be shared between the accountable institutions when one or more of them is contemplating the reporting of a suspicion to the FIC". Secondly, it is justified by "the impact such sharing may have on the FIC's operations".[143] However, the Explanatory Memorandum states that, once the FIC is notified of the sharing of information for the purposes of section 29 reporting, the FIC "will work with the relevant institutions to facilitate the making of such a report". The decisions regarding reporting and coordination – aimed at preventing miscommunication that could lead to a failure to report at all – remain the responsibility of the relevant AIs.

Both notifications under subsections (5) and (7) must adhere to the format specified by the FIC.[144] The AI is required to maintain a record of the information shared and received, along with the purpose of the information sharing request.[145] This latter requirement is necessary to ensure supervisory compliance with *FICA* and its regulations.[146]

5.5.6 De-risking and defensive reporting

Although the *Draft Amendments* do not directly address this issue, the Explanatory Memorandum cautions that information sharing may reveal information regarding an AI's client, requiring a re-assessment of the ML/TF risks associated with that client. This re-assessment should incorporate any

142 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

143 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

144 Section 27E(9) of the *Draft Amendments*.

145 Section 27E(10) of the *Draft Amendments.*

146 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

additional information within the broader context of all available information. The Memorandum further warns against over-reliance on potentially inaccurate third-party information, as this could lead to decisions to limit or deny transactions with the client. AIs "should avoid" denying or restricting business relationships based solely on information shared in the context of reporting under section 29, as this may cause inappropriate de-risking.

FATF defines de-risking as the practice whereby FIs terminate or restrict business relationships with clients to avoid rather than manage risk, in alignment with the FATF's risk-based approach. De-risking may interfere with the FIC's ability to monitor a person's financial activities, as it is argued that keeping criminals within the financial system allows for better oversight than excluding them and driving them to the informal or dark economy.[147]

Information shared across multiple AIs may alert an AI to the fact that a section 29 report has been filed or is being contemplated against its client, which could exacerbate the defensive reporting of suspicious or unusual transactions. According to FATF, defensive reporting occurs when an FI feels obliged to file an STR on a customer after learning that other FIs have done so.[148] Defensive reporting obscures true intelligence, overwhelms FIUs, hinders their ability to detect authentic criminal activity, and may result in regulatory scrutiny and potential penalties.[149]

5.6 The 2024 Draft General Laws (AML and CFT) Amendment Bill

The 2024 *Draft General Laws (AML and CFT) Amendment Bill*, published on 19 December 2024 for public comment, makes no reference to P2P.[150] Although South Africa has been removed from the FATF greylist, the next round of mutual evaluations starts in 2026, during which progress on the implementation of P2P could yield positive outcomes.[151]

6 Comparison of selected international P2Ps

The comparison examines the aims, establishment and enabling environments of these P2P frameworks, including their protection of

147 National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf.

148 FATF 2014 https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html.

149 Kazlauskas 2023 https://amlyze.com/sars-suspicious-or-defensive-reports/.

150 GN 5683 in GG 51772 of 13 December 2024 (*Draft General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Bill*, 2024).

151 FATF 2017 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf; FATF 2025 https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2025.html.

personal information, maintenance of confidentiality and integrity, the types of information that may be shared, and public sector involvement.

6.1 Aim, establishment and enabling legislation

The *USA PATRIOT Act*, which was enacted in September 2002 in response to the September 11 attacks, includes a unique provision known as section 314(b). This section enables eligible entities to voluntarily share information with the federal government with the aim of identifying and reporting activities that may involve ML/TF and related crimes. It provides a safe harbour from litigation related to information shared via a P2P.[152]

Singapore's *Financial Services and Markets (Amendment) Act* 11 of 2023, which is effective from April 2024, added Part 4 to the *Financial Services and Markets Act* (*FSM Act*). This amendment establishes a P2P framework for prescribed FIs to "permit the disclosure, publication and sharing of certain information (despite any restriction … imposed by law, contract or rules of professional conduct) between [persons identified in subsection 2]", for the purposes of preventing and detecting ML/TF/PF, according to section 28A(1).[153]

This led to the establishment of COSMIC, a digitalised secure central platform, a global first, which allows FIs to share information about customers who exhibit multiple "red flags" that may indicate potential financial crime concerns, if stipulated thresholds are met.[154] Launched in April 2024, COSMIC was co-developed by the central bank, the Monetary Authority Singapore (MAS), and six major banks,[155] focussing on three key financial crime risks in commercial banking: the misuse of legal persons, trade-based ML, and PF.

The Netherlands' TMNL was a voluntary private initiative founded by five banks in the Netherlands, all of which were shareholders in TMNL, a legal entity focussing on ML/TF.[156] It was founded in July 2020 and prioritised the combating of ML/TF.[157] However, its activities have been "wound down" since July 2024 in anticipation of the European AML Regulation, which is set to be enacted in July 2027. This development will significantly reshape

---

152 FinCEN 2013 https://www.fincen.gov/system/files/shared/sar_tti_23.pdf; FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

153 Section 28A of the *Financial Services and Markets Act* 18 of 2022 (the *FSM Act*).

154 Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023; MAS 2025 https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic.

155 MAS 2024 https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform.

156 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

157 TMNL 2022 https://tmnl.nl/app/uploads/2022/10/TMNL-Legislaton-EN.pdf.

TMNL's future operations, prompting it to restructure and discontinue in its current form.[158] During its full operation, TMNL did not have dedicated enabling legislation but was subject to the *Anti-Money Laundering and Anti-Terrorist Financing Act*, 2008 and the EU GDPR.[159]

The FIs participating in TMNL faced criticism for their lenient approach to the protection of banking secrecy when sharing client information. This included using codes instead of clients' names or sharing information even when no high risk for illegal transactions had been identified. Critics argued that the current practice violated the presumption of innocence.[160]

The Estonia AML Bridge, which was established in October 2020, is a collaborative information and data exchange platform for FIs created by a fintech company, Salv. Piloted by four banks with government support, it initiated almost 1,200 joint investigations within nine months.[161] The platform allows participants to securely share information in real time to detect and prevent ML/TF and related crimes through advanced technology and secure data-sharing solutions.[162] Salv Bridge also facilitates rapid cross-border communication, enabling participants to collaborate on fraud investigations, share typologies and recover stolen funds before they can be laundered.[163] Salv's platforms are now used across 14 countries. Each participant, acting as a data controller, must have a lawful basis under the GDPR for sharing information.

Estonia's *ML/TF Prevention Act* 174 of 2017[164] permits limitations on certain data protection rights, recognising that AML/CFT/CPF efforts serve the public interest. Section 16 of the Act allows FIs to exchange personal data for cooperation purposes, while section 48 permits the restriction of certain data subject rights in this context.

6.1.1 Summary on aim, establishment and enabling legislation

158 TMNL 2024 https://tmnl.nl/en/article/transaction-monitoring-netherlands-adapts-its-working-method-to-new-european-legislation/.

159 TMNL 2022 https://tmnl.nl/app/uploads/2022/10/TMNL-Legislaton-EN.pdf.

160 Nalog.NL 2024 https://www.nalog.nl/en/news/2024/08/06/svorachivaetsya-programma-proverki-bankovskix-tranzakcij-tmnl/.

161 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

162 Liive 2021 https://investinestonia.com/estonian-fintech-salv-gives-banks-secure-information-exchange/.

163 FinTech Global 2025 https://fintech.global/2025/11/05/salv-expands-bridge-network-as-lithuania-joins-fight-on-fraud/.

164 Originating from *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA Relevance)* [2015] OJ L 141 73.

It is imperative that P2P information sharing is supported by a clear legal basis, as the absence of such a foundation may expose participants to legal and reputational risks, including civil damages, defamation, AML tipping-off transgressions, de-risking, and impediments to data-privacy and competition law.[165] Enabling legislation does not necessarily need a dedicated law or supervisory instrument that permits P2P; it could also take the form of an exemption or exception to existing restrictions on information sharing. However, explicit enabling legislation, subject to oversight from a data-privacy protection authority, will provide legal certainty and encourage active participation from the private sector, addressing any legal, reputational and business concerns participants may have.[166]

The US's section 314(b) of the *PATRIOT Act*, Singapore's COSMIC and the Estonian AML Bridge operate under clear legislative mandates for P2P information sharing. Conversely, significant changes to TMNL's legislative framework contributed to the winding down of its activities. The AML Bridge is notable in that it was developed in the private sector and subsequently adopted by FIs with government approval.

In South Africa the enactment of section 41A(3) of *FICA* formally introduced P2P into the AML regime applicable to AIs and section 29 reporting duties, while complying with the requirements of personal information protection. *Draft Amendments to the ML Regulations* aimed at establishing the foundation for the anticipated P2P framework were issued for public comment in September 2023, but no further progress has been reported.

6.2 Who may share what information and how?

FIs subject to the Financial Crime Enforcement Network of the USA (FinCEN) AML programme requirements, along with any associations of such institutions, are eligible to share information under section 314(b) of the *PATRIOT Act*.[167] These include casinos, banks, card clubs, brokers or dealers in securities, money services businesses, insurance companies, mutual funds, dealers in precious stones, jewels or metals, futures commission merchants, introducing brokers, loan or finance companies, government housing-sponsored enterprises, and operators of credit card

165 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

166 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

167 FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

systems[168] – enabling cross-industry sector information sharing.[169] Disclosure under section 314(b) is voluntary.[170]

Protection under section 314(b) is granted upon registering with FinCEN's Secure Information Sharing System (SISS). Before sharing information institutions must take reasonable steps to verify the recipient's registration as a 314(b) participant on the real-time SISS participant list. Participants may share information pertaining to "individuals, entities, organisations, and countries" when they have "a reasonable basis to believe" that it concerns activities that may involve ML/TF, even without conclusive evidence or a defined transaction.[171] This includes attempted transactions, recruitment efforts (e.g., a money mule scheme), and a range of "specified unlawful activities" listed in 18 U.S.C § 1956, encompassing various fraudulent and other criminal activities, which are predicate crimes to ML.[172]

Furthermore, section 314(b) permits the sharing of personally identifiable information and does not restrict the type or medium of information that can be shared, e.g., video surveillance or cyber-related data such as IP addresses. Information sharing can occur verbally or in writing. FinCEN encourages FIs to note in SAR narratives when section 314(b) information sharing contributed to the report, in order to help track the benefits of the programme. In 2020 over 7,000 FIs participated in the section 314(b) programme, with 17,384 SAR narratives referencing the use of section 314(b), either as the sender or the recipient.[173]

Participation in COSMIC is voluntary, but responding to an information request is compulsory. In the future, both participation and responding will be compulsory. Currently only six banks participate, but plans are in place to expand participation to other FIs.[174] COSMIC allows its participants to securely and conditionally share information regarding ML/TF/PF related to customers who exhibit multiple "red flags", provided stipulated thresholds are met.[175] Participants are allowed to share "risk information", which encompasses details about the relevant parties, their relationship with the

168 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

169 FinCEN 2013 https://www.fincen.gov/system/files/shared/sar_tti_23.pdf 42.

170 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

171 FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

172 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

173 FinCen 2022 https://www.fincen.gov/system/files/shared/314(b)%20Infographic%20-%20Participation%20and%20Reporting%20CY2020.pdf.

174 Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023.

175 Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023; MAS 2025 https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic.

FI, transactions they are party to, relevant high-risk indicators and the FIs' analysis thereof, any other information the FI has obtained, including analysis to assess the relevant parties' involvement in ML/TF/PF, any documents that can serve as evidence of risk information, and any other information MAS may prescribe.[176]

Information is shared through COSMIC in three ways.[177] First, when a customer displays red-flag behaviour that crosses the stipulated threshold, an FI may request risk information (a Request message) from other FIs linked to the customer or transactions to investigate unusual activities. Requests must clarify specific concerns regarding the observed red flags and include context for assessment purposes. If the receiving FI deems the request valid and useful, it should respond within a reasonable period and may use the information to assess its own customer.

Second, if an FI detects multiple red flags regarding a customer's behaviour that exceed a higher stipulated threshold – suggesting possible involvement in illicit activity – the FI must proactively provide information (a Provide message) to other FIs connected to the customer or transaction. This should outline the context, observed red flags, and relevant risk information. Upon receiving such information, the receiving FI must conduct an AML/CFT assessment of its own customer within a reasonable time.

Third, when a customer's behaviour meets the higher threshold of red flags, and the FI has filed an STR and terminated the relationship, the FI must place an "Alert" on the customer in the COSMIC watchlist. The alert should include the reasons for concern, the red flags observed, and relevant risk information, which participating FIs are expected to consider in their own AML/CFT assessments.[178]

During its full operation TMNL only shared clients' transaction data, including account numbers, transaction types and amounts, IDs, account and client types, and client industries regarding ML.[179] Due to the pseudonymisation methodology applied, TMNL was unable to identify

---

176 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

177 MAS 2021 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf.

178 MAS 2021 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf.

179 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-in-the-fight-against-financial-crime.pdf.coredownload.pdf; Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

individual clients from the datasets provided. Consequently, TMNL could alert banks to the transaction patterns it observed only. TMNL pooled and connected the datasets of the participating banks in analytical models on a highly secure IT platform. Alerts sent to participants contained a unique identifier that only the receiving participant could match to its own client records.[180]

Participation in the Estonian AML Bridge is voluntary, and information is shared to detect and prevent ML/TF, sanction use cases and other financial crimes.[181] The initiative is operated by Salv and was piloted by Estonia's four largest banks (representing a 90% share of the domestic market), with the full support of Estonia's Financial Supervision and Resolution Authority, Data Protection Inspectorate, and FIU. It now includes all 10 banks and several non-bank entities, for instance, non-bank fintechs, money service businesses, and payment service providers.[182] The platform is primarily used for sharing transaction-related data in near real time. Information is shared using configurable scenario templates tailored to the suspected offence and participants involved. These templates assist in defining inputs required to identify subjects, including account numbers, transaction IDs, customer names, dates of birth, payment reasons, sources of wealth, risk levels, copies of documents, etc.[183] The speed of the tooling has proven a major factor in successful fraud recalls, with three of the most active participants resolving over 50 per cent of cases in under 10 minutes.[184]

6.2.1 Summary on who may share what information and how

In the USA P2P participation is voluntary, with FinCEN actively encouraging involvement. In COSMIC participation is voluntary, but responding to requests is compulsory, while it is anticipated that participation will eventually become compulsory. Participation is voluntary in the AML Bridge, which commendably involves all banks. Participation in TMNL was also voluntary.

For the AML/CTF/PF regime to be effective and efficient, as demonstrated by the purpose and functioning of FATF, it is imperative that as many role players as possible – both domestically and internationally – adhere thereto.[185] Limited participation in a P2P system may impede its effectiveness, as unscrupulous competitors who choose not to participate

180 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.
181 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.
182 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.
183 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.
184 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.
185 FATF 2024 https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness.html.

might take risks to gain a market share advantage.[186] Although participation in the envisioned SA model is voluntary, measures should be implemented to encourage involvement, such as through industry associations and by promoting a stance against engaging with illicit clients or dirty money.

The US model involves a broad range of private sector participants, enabling rich cross-sectoral information sharing. Currently, COSMIC's participation is limited to six banks but it will eventually be accessible to all FIs. TMNL included banks only, but it will undergo a complete overhaul, while the AML Bridge also includes private sector participants beyond banks.

The proposed SA framework will allow for AIs, as defined by *FICA* Regulations, to participate, enabling a broad range of cross-sectoral information sharing. While recognising the perils of involving too many participants and the potential for misuse of the P2P, it is recommended that participation be expanded to include role players who would add valuable sector-specific information, such as the telecommunications industry, as illustrated by COMRiC. Public participation should also extend to the IR, as seen in Estonia, to address privacy concerns that potential private sector participants may have.

The TMNL, the AML Bridge and COSMIC all utilise a secure electronic platform for information sharing. While the US model also employs an electronic platform, it additionally permits oral information sharing. The prospective SA model suggests using an electronic platform, although it is proposed that it should also provide for oral information sharing in urgent cases, such as phishing attacks compounded by instantaneous payments, or life-threatening kidnappings for ransom.[187] The Explanatory Memorandum recommends that participating AIs develop a platform for information exchange, engaging experienced service providers with established and reliable products, such as Salv, to minimise development costs and save time (given the need for expedient P2P implementation), provided that administration rights and data protection are maintained.

The format and type of information shared by each P2P system vary, as well as the type of crime addressed. The US model clearly defines the format and type of information that may be shared, including attempted transactions, recruitment efforts and a range of specified unlawful activities related to ML/TF, as well as predicate crimes, even in the absence of conclusive evidence or a defined transaction. There are no restrictions on the type or medium of information that can be shared.

---

186 De Koker *et al* 2025 *Money Laundering* 7.

187 Libera 2025 https://businesstech.co.za/news/lifestyle/831182/new-crime-tactic-in-south-africa-thats-so-bad-other-countries-are-warning-their-citizens-about-it/.

COSMIC may share risk information (identifying details, transactional information, risk indicators and supporting documentation) only if a client exhibits red flag behaviour concerning ML/TF/PF. TMNL participants shared pseudonymised information on account numbers, transaction types and amounts, IDs, account and client types, and client industries related to ML. The AML Bridge employs a template that includes the account number, transaction ID, and customer name, full name, date of birth, payment reason, source of wealth, risk level, and supporting documents relating to ML/TF/PF and other financial crimes.

The SA model currently allows information sharing only for the purposes of section 29 reporting, which impedes the potential value of the P2P. It is recommended that the scope of shareable information be broadened to encompass a wider range of crimes, as seen in the comparator countries, and that the type of information be defined within their respective Risk Management Compliance Programmes – keeping it sufficiently broad to accommodate the circumstances of each case.

6.3 Data security and the protection of privacy

Section 314(b) of the *PATRIOT Act* mandates that P2P participants maintain adequate procedures to protect the security and confidentiality of all shared information, using it only for purposes set therein, namely identifying and reporting activities that may involve ML/TF, assisting in AML compliance, and determining whether to establish or maintain an account or engage in a transaction.[188] Participants are not authorised to share an SAR itself or disclose information that would reveal the existence of an SAR; however, those sharing information pursuant to section 314(b) may collaborate to file joint SARs.

Prior to sharing information under this section, participants must first register on the FinCEN SISS programme and take reasonable steps, such as checking the FinCEN 314(b) participant list, to verify that the other participant is also a 314(b) registrant. Section 314(b) and its implementing regulations impose no limitations on the sharing of personally identifiable information under the section 314(b) safe harbour.[189] FinCEN cautions that human oversight is crucial during information exchange to ensure that decision making is fair and based on accurate data. This includes designating a contact person for dealing with section 314(b) communications.[190]

188 FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.
189 FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.
190 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

Singapore's *Personal Data Protection Act* 26 of 2012 (*PDPA*) provides a legislative route allowing other laws to prevail over *PDPA* requirements,[191] of which the *Financial Services and Markets (Amendment) Act* of 2023 (the *FSM Amendment Act*),[192] effective from April 2024, is relevant for COSMIC.[193] COSMIC is designed to allow FIs to share risk-related information about "relevant parties" suspected of ML/TF/PF, if stipulated thresholds are met, and without tipping off potential criminals. "Relevant party" is defined in section 28B of the *FSM Act* as a person who is a "customer, seeks to be a customer or has been a customer" of the prescribed FI.[194] Strict safeguards are in place to protect legitimate customers. Information may be shared only among "persons" defined in section 28A(2), specifically any bank in Singapore or qualifying FI, the MAS, any Suspicious Transaction Reporting Officer as defined in section 2(1) of the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act*,1992 or any other person defined in Schedule Three of the Act. Any information disclosed, published or shared under the *FSM Act* may be used only for a purpose listed in section 28A(1), namely the prevention and detection of ML/TF/PF, except as otherwise provided.[195]

The required thresholds refer to the stipulation that information may be shared only after determining that a customer meets the materiality risk thresholds based on specific red flags.[196] Information may not be shared regarding legitimate customers who do not exhibit higher-risk behaviours. FIs should assess whether a customer's profile warrants concern before sharing information, consider other information sources rather than solely relying on COSMIC information, allow customers to explain observed behaviours, and ensure the accuracy and completeness of the information shared.[197] The responding FIs must also assess whether the requested information will assist in the assessment and determination of the ML/TF/PF risk concerns before sharing.

The COSMIC legislative framework enforces confidentiality and data accuracy, and restricts disclosures to clearly defined, appropriate purposes such as operational needs, group-wide risk management, and regulatory requirements. Information must be securely stored and encrypted, never

191 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

192 Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023.

193 Singapore Statutes Online 2023 https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628.

194 MAS 2025 https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic.

195 Section 28A(3) of the *FSM Act*.

196 Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023.

197 MAS 2025 https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic.

kept on personal devices unless absolutely necessary, and actions involving sensitive data must be logged. FIs must comply with the MAS's Technology Risk Management Guidelines and Cyber Hygiene requirements.[198]

TMNL primarily worked with business clients' data and, due to GDPR rules and laws, TMNL had limited access to personal data associated with companies being processed.[199] As part of a "privacy by design" approach, participating banks (the data controllers) and TMNL (the data processor) conducted a Data Protection Impact Assessment to assess compliance with GDPR principles. Data privacy and security safeguards was formalised in a user agreement, and privacy considerations for each analytical model were documented separately.

In TMNL, the processing of data was grounded in the banks' legitimate interest in fulfilling their AML obligations, as supported by the National Action Plan against ML. Data quality analysis and remediation processes were performed by both banks and TMNL to assess the suitability of using data items in analytical models. Measures were implemented to ensure high-quality data processing, which included keeping data within TMNL's Information Technology platform that adhered to strict security standards and undergoes continuous monitoring.[200] Analytical models were governed by a model risk framework that ensured their validity, fairness and transparency.[201] Additionally, TMNL employed encryption and privacy-preserving techniques to pseudonymise data and achieve data minimisation.[202]

The AML Bridge is encrypted and compliant with data protection regulations, following a full regulatory assessment with input from pilot participants and regulators/supervisors, along with testing on synthetic data.[203] Participants can share information under GDPR Article 6.1(e) on the grounds of "compliance with the law" or "legitimate interest".[204]

198 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

199 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

200 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

201 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

202 Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf.

203 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

204 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

Estonia's *ML/TF Prevention Act* imposes certain limitations on data privacy protection rights, since AML/CFT/CPF activities are deemed to be in the public interest.[205] Section 16 permits FIs to share personal data for collaboration purposes,[206] whereas section 48 allows for restrictions on certain privacy rights of a data subject based on the public interest of AML/CFT/CPF activities.[207] Participants sign a Data Processing Addendum, which is a contract between the participant and Salv, to ensure data protection in compliance with the GDPR.[208]

The platform ensures strong data security through a comprehensive security management system that includes multifactor authentication, IP whitelisting, encryption, disaster recovery protocols, and audit logs. Independent annual security testing is conducted, and participants may perform their own penetration testing. The AML Bridge employs end-to-end password-based encryption, securing messages with public-private key pairs. Decryption requires access to a private key protected by a secondary password, which remains inaccessible to the platform provider and any other party.[209]

6.3.1 Summary on data security and the protection of privacy

In all the comparator frameworks, including the envisioned SA model, the preservation of data security and the protection of privacy are paramount. Specific information may be shared only among qualifying parties through secure channels and for designated purposes in terms of legislative frameworks. Legislation that protects participants in sharing information is also crucial, as it encourages participation by removing the risk of civil and criminal actions stemming from breaches of privacy and confidentiality.

However, the level of detail provided differs. The proposed SA model places strong emphasis on adherence to *POPIA*, although it remains unclear whether and to what extent P2P, or the sharing of information between AIs for the purposes of section 29 reporting, will qualify for exemption. Clarity in this regard, either via specific legislation or the discretion afforded to the IR, with the recommended involvement of the IR in the SA P2P framework, is

205 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

206 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

207 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

208 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf; Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

209 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

required, as the provisions of *POPIA* may otherwise severely limit the sharing of information.

6.4 Public sector involvement and oversight

Public sector involvement with the US's section 314(b) P2P is minimal, as participating FIs must register with FinCEN, but neither they nor any other government agency can access shared information unless referenced in an STR.[210]

Singapore's COSMIC is a public-led initiative co-developed with the private sector, owned and operated by MAS, and fully integrated into its supervisory and surveillance framework. Singapore's FIU, the Suspicious Transaction Reporting Office (STRO), which falls under the Singapore Police Force, has access to COSMIC data for analytical purposes.[211] Banks collaborate closely with government partners to align on strategic and regulatory matters and work with law enforcement to incorporate AML intelligence and typologies into their multibank detection model.[212]

TMNL's public sector involvement occurred only when information shared between banks needed to be reported to the Dutch FIU.[213]

Estonia's AML Bridge has limited public sector involvement but has obtained full support from the FIU, as well as the Data Protection Inspectorate and the Financial Supervision and Resolution Authority, which act as advisors for the AML Bridge.[214] Law enforcement agencies and FIUs can access the AML Bridge platform to collaborate with FIs on resolving complex ML investigations.[215]

6.4.1 Summary on public sector involvement and oversight

Each comparator country exhibits varying degrees of public sector involvement. FinCEN is only engaged in registering FIs for section 314(b) information sharing. COSMIC has a notable public sector involvement, as MAS owns, operates and has full access to the COSMIC platform, along with law enforcement agencies and the FIU. TMNL only involved the public

---

210 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf; FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

211 Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf.

212 FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

213 Rene and Lambert-Porter 2025 https://www.ropesgray.com/en/insights/alerts/2020/12/transaction-monitoring-netherlands-a-novel-solution-to-the-banking-industrys-aml-puzzle.

214 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

215 Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf.

sector when reporting a suspicion to the FIU. Law enforcement and the FIU also have access to the AML Bridge, with the Data Protection Inspectorate and Financial Supervision and Resolution Authority supporting the AML Bridge as advisors.

The SA model requires participants to notify the FIC after information sharing, allowing the FIC to assist AIs in making section 29 reports and staying informed about information-sharing initiatives that may affect its operations. This requirement could impose additional administrative burdens and costs on participants, potentially outweighing the incentives for participation. Information sharing can be reported to the FIC in the narrative of subsequent STRs filed with the FIC, akin to the US model.

7 Conclusion

Access to real-time, reliable, comprehensive and cross-sectoral information lies at the core of preventing, detecting and disrupting economic crime. Effective, efficient and legally compliant information- sharing partnerships that leverage the skills, capacity and data available in diverse private sector entities are critical to disrupting not only ML/TF/PF but also the ever-evolving scourge of economic crime, as demonstrated by the literature and practical successes of the P2P frameworks analysed.

Enabling legislation has opened the door for P2P information sharing in South Africa. The concomitant *Draft Amendments* to the relevant Regulations, aimed at embodying these functionalities, are still in progress. The comparator P2P frameworks show that regulatory confirmation is imperative to establishing a safe harbour for cross-sectoral voluntary P2P participation, ensuring that reputational and legal risks are mitigated, while fostering trust among participants and relevant public role players – all while addressing the privacy concerns of customers.

Participation in the envisioned SA model is voluntary, but measures should be implemented to encourage involvement. Participation should be expanded to include, for example, telecommunications companies, as they can provide crucial cross-industry information. The proposed requirement to notify the FIC upon information sharing may impose administrative burdens on AIs, potentially discouraging participation, and should therefore be reconsidered.

Furthermore, the SA P2P model currently focusses solely on section 29 reports under *FICA*. This scope needs to be broadened to encompass a wider range of crimes. In the interest of time and cost-effectiveness, it is proposed that participants tasked with establishing the P2P platform consider adopting an existing platform, such as Salv, used by the AML Bridge. A legally compliant, secure, effective and efficient P2P is urgently

required as an additional tool, supplementing existing collaborative efforts, to enhance South Africa's capacity to combat economic crime.

Bibliography

Literature

De Koker *et al* 2025 *Money Laundering*
De Koker L *et al* (eds) *Money Laundering and Terrorist Financing Law and Compliance in South Africa* (LexisNexis Cape Town 2025)

De Koker and Casanovas "'De-risking', De-banking and Denials of Bank Services"
De Koker L and Casanovas RP "'De-risking', De-banking and Denials of Bank Services: An Over-compliance Dilemma?" in Goldbarsht D and De Koker L (eds) *Financial Crime, Law and Governance: Navigating Challenges in Different Contexts* (Springer Cham 2024) 45-70

Goldbarsht "Private to Private"
Goldbarsht D "Private to Private: Measures to Enhance Private-Private Information Sharing to Combat Financial Crime?" unpublished paper delivered at the *South African Financial Crime Symposium* (4-5 March 2025 Pretoria)

Harris "Fraud Risk Management"
Harris N "Fraud Risk Management" Unpublished lecture presented at the North-West University (30 August 2025 Online via MS Teams)

Kruger *Organised Crime and Proceeds of Crime Law*
Kruger A *Organised Crime and Proceeds of Crime Law in South Africa* 2nd ed (LexisNexis Durban 2013)

Malahleka 2024 *PELJ*
Malahleka M "The Problem of Trans-border Information Flows in the Protection of Personal Information" 2024 *PELJ* 1-40 https://doi.org/10.17159/1727-3781/2024/v27i0a14296

Mkhabela "South Africa and the Capture of the Executive"
Mkhabela M "South Africa and the Capture of the Executive: Undermining Transformation?" in Meirotti M and Masterson G (eds) *State Capture in Africa Old Threats, New Packaging?* (EISA Johannesburg 2018) 119-130

Onwuegbuzie and Weinbaum 2017 *The Qualitative Report*
Onwuegbuzie AJ and Weinbaum RK "A Framework for Using Qualitative Comparative Analysis for the Review of the Literature" 2017 *The Qualitative Report* 359-372 https://doi.org/10.46743/2160-3715/2017.2175

Pedersen *Investigator's Guide to Open-Source Intelligence*
Pedersen C *Investigator's Guide to Open-Source Intelligence* (TCG Forensics Cape Town 2019)

Pickvance 2001 *Journal of Housing and the Built Environment*
Pickvance CG "Four Varieties of Comparative Analysis" 2001 *Journal of Housing and the Built Environment* 7-28 https://doi.org/10.1023/A:1011533211521

SAFPS "South African Fraud Prevention Services"
SAFPS "South African Fraud Prevention Services" (PowerPoint presentation 2025) (on file with the author)

Swanepoel *Financial and Moral Perspective*
Swanepoel AP *A Financial and Moral Perspective of the Impact of Economic Crime on Taxation* (PhD Tax-dissertation North-West University 2013)

Legislation

Estonia

Money Laundering and Terrorist Financing Prevention Act 174 of 2017

European Union

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA Relevance) [2015] OJ L 141 73

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing pf Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance) [2016] OJ L 119 1

The Netherlands

Anti-Money Laundering and Anti-Terrorist Financing Act, 2008

Singapore

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act,1992

Financial Services and Markets Act 18 of 2022

Financial Services and Markets (Amendment) Act 11 of 2023

Personal Data Protection Act 26 of 2012

South Africa

Drugs and Drugs Trafficking Act 140 of 1992

Financial Intelligence Centre Act 38 of 2001

General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 22 of 2022

Prevention and Combating of Corrupt Activities Act 12 of 2004

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004

Proceeds of Crime Act 76 of 1996

Prevention of Organised Crime Act 121 of 1998

United States of America

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 56 of 2001

Government publications

GN R1595 in GG 24176 of 20 December 2002 (*Money Laundering and Terrorist Financing Control Regulations*)

GN R1062 in GG 41154 of 29 September 2017 (*Money Laundering and Terrorist Financing Control Regulations*)

GN 5683 in GG 51772 of 13 December 2024 (*Draft General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Bill*, 2024)

International instruments

United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)

United Nations Convention Against Transnational Organised Crime (2000)

United Nations Convention Against Corruption (2003)

Internet sources

Alessa 2024 https://alessa.com/blog/how-to-reduce-aml-false-positives/
Alessa 2024 *How to Reduce AML False Positives* https://alessa.com/blog/how-to-reduce-aml-false-positives/ accessed 8 October 2025

Basel Institute on Governance 2018 https://baselgovernance.org/sites/default/files/2019-02/basel_aml_index_10_09_2018.pdf
Basel Institute on Governance 2018 *Basel AML Index 2018 Report* https://baselgovernance.org/sites/default/files/2019-02/basel_aml_index_10_09_2018.pdf accessed 25 September 2025

Basel Institute on Governance 2024 https://baselgovernance.org/sites/default/files/2024-11/2024%20Basel%20AML%20Index%20report.pdf
Basel Institute on Governance 2024 *Basel AML Index 2024: 13th Public Edition. Ranking Money Laundering Risks Around the World* https://baselgovernance.org/sites/default/files/2024-11/2024%20Basel%20AML%20Index%20report.pdf accessed 7 September 2026

Basel Institute on Governance 2025 https://baselgovernance.org/basel-aml-index/methodology/indicators
Basel Institute on Governance 2025 *Indicators Used in the Basel AML Index* https://baselgovernance.org/basel-aml-index/methodology/indicators accessed 18 March 2025

COMRiC 2023 https://comric.co.za/wp-content/uploads/2023/06/COMRiC-Website-Privacy-Notice-130623.pdf
Communications Risk Information Centre 2023 *Website Privacy Notice* https://comric.co.za/wp-content/uploads/2023/06/COMRiC-Website-Privacy-Notice-130623.pdf accessed 10 August 2025

COMRiC 2025 https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf
Communications Risk Information Centre 2025 *Telecommunications Sector Report 2025* https://comric.co.za/reports/COMRiC_Sector%20Report_Interactive.pdf accessed 10 August 2025

Deloitte 2024 https://www.deloitte.com/content/dam/assets-zone2/uk/en/docs/services/financial-advisory/2024/fa-article75-thought-leadership-final.pdf
Deloitte 2024 *Article 75: A New Opportunity to Fight Crime Effectively* https://www.deloitte.com/content/dam/assets-zone2/uk/en/docs/services/financial-advisory/2024/fa-article75-thought-leadership-final.pdf accessed 7 November 2025

DoJCD 2016 https://www.justice.gov.za/m_speeches/2016/20161027-dm-SABRIC.html
Department of Justice and Constitutional Development 2016 *Address by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP, at the SABRIC Stakeholder Dinner, Held at Shepstone Gardens, Johannesburg, 27 October 2016* https://www.justice.gov.za/m_speeches/2016/20161027-dm-SABRIC.html accessed 27 September 2025

Europol 2021 https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
Europol 2021 *European Union Serious and Organised Crime Threat Assessment a Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime* https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf accessed 12 November 2025

Europol 2025 https://www.europol.europa.eu/crime-areas/economic-crime
Europol 2025 *Economic Crime* https://www.europol.europa.eu/crime-areas/economic-crime accessed 24 August 2025

FATF 2014 https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html
Financial Action Task Force 2014 *FATF Clarifies Risk-based Approach: Case-by-Case, not Wholesale De-risking* https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html accessed 7 October 2025

FATF 2017 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf
Financial Action Task Force 2017 *FATF Guidance: Private Sector Information Sharing* https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf accessed 11 July 2025

FATF 2022 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf
Financial Action Task Force 2022 *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf accessed 25 June 2025

FATF 2023 https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
Financial Action Task Force 2023 *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html accessed 26 July 2025

FATF 2023 https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html
Financial Action Task Force 2023 https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-february-2023.html accessed 25 September 2025

FATF 2024 https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness.html
Financial Action Task Force 2024 *An Effective System to Combat Money Laundering and Terrorist Financing* https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness.html accessed 10 November 2025

FATF 2024 https://www.fatf-gafi.org/en/the-fatf/mandate-of-the-fatf.html
Financial Action Task Force 2024 *Mandate of the Financial Action Task Force* https://www.fatf-gafi.org/en/the-fatf/mandate-of-the-fatf.html accessed 25 September 2025

FATF 2025 https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf.coredownload.inline.pdf
Financial Action Task Force 2025 *Methodology for Assessing Technical Compliance with the FATF Recommendation and the Effectiveness of AML/CFT/CPF Systems* https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf.coredownload.inline.pdf accessed 10 October 2025

FATF 2025 https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2025.html
Financial Action Task Force 2025 *Jurisdictions Under Increased Monitoring – 24 October 2025* https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2025.html accessed 7 November 2025

FATF 2025 https://www.fatf-gafi.org/en/publications/Fatfgeneral/pscf-march-2025.html
Financial Action Task Force 2025 *Private Sector Collaborative Forum Reinforces Importance of Public-Private Collaboration in the Fight Against Financial Crime* https://www.fatf-gafi.org/en/publications/Fatfgeneral/pscf-march-2025.html accessed 9 July 2025

FIC date unknown https://www.fic.gov.za/about/
Financial Intelligence Centre date unknown *The Financial Intelligence Centre* https://www.fic.gov.za/about/ accessed 25 September 2025

FIC 2022 https://www.fic.gov.za/wp-content/uploads/2023/09/2022.12-CG-FIC-Act-reference-guide.pdf
Financial Intelligence Centre 2022 *Reference Guide for All Accountable Institutions* https://www.fic.gov.za/wp-content/uploads/2023/09/2022.12-CG-FIC-Act-reference-guide.pdf accessed 25 June 2025

FinCEN 2013 https://www.fincen.gov/system/files/shared/sar_tti_23.pdf
Financial Crimes Enforcement Network of the USA. 2013. The SAR Activity Review: Trends, Tips, *and Issues. Issue 23* https://www.fincen.gov/system/files/shared/sar_tti_23.pdf accessed 9 November 2025

FinCEN 2020 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
Financial Crime Enforcement Network of the USA 2020 *Section 314(b) Fact Sheet* https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf accessed 28 June 2025

FinCen 2022 https://www.fincen.gov/system/files/shared/314(b)%20Infographic%20-%20Participation%20and%20Reporting%20CY2020.pdf
Financial Crime Enforcement Network of the USA 2022 *314(b) Participation and Reporting* https://www.fincen.gov/system/files/shared/314(b)%20Infographic%20-%20Participation%20and%20Reporting%20CY2020.pdf accessed 7 September 2026

FinTech Global 2025 https://fintech.global/2025/11/05/salv-expands-bridge-network-as-lithuania-joins-fight-on-fraud/
FinTech Global 2025 *Salv Expands Bridge Network as Lithuania Joins Fight on Fraud* https://fintech.global/2025/11/05/salv-expands-bridge-network-as-lithuania-joins-fight-on-fraud/ accessed 8 November 2025

Global Initiative Against Transnational Organized Crime 2023 https://ocindex.net/report/2023/0-3-contents.html
Global Initiative Against Transnational Organized Crime 2023 *Global Organized Crime Index 2023: A Fractured World* https://ocindex.net/report/2023/0-3-contents.html accessed 7 September 2026

Home Office and HM Treasury 2016 https://assets.publishing.service.gov.uk/media/5a74e52440f0b65c0e8455bd/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf
Home Office and HM Treasury 2016 *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* https://assets.publishing.service.gov.uk/media/5a74e52440f0b65c0e8455bd/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf accessed 24 October 2025

ICB 2025 https://www.saicb.co.za/pages/company-history
Insurance Crime Bureau 2025 *Company History* https://www.saicb.co.za/pages/company-history accessed 6 October 2025

ICB 2025 https://www.saicb.co.za/pages/company-profile
Insurance Crime Bureau 2025 *Committed to Insurance Fraud Detection and Prevention* https://www.saicb.co.za/pages/company-profile accessed 6 October 2025

ICB 2025 https://www.saicb.co.za/pages/membership
Insurance Crime Bureau 2025 *Working Together to Detect and Prevent Insurance Policy Fraud* https://www.saicb.co.za/pages/membership accessed 6 October 2025

ICB 2025 https://www.saicb.co.za/uploads/files/Insurance-Crime-Bureau-2024-Annual-Report.pdf
Insurance Crime Bureau 2025 *Annual Report* https://www.saicb.co.za/uploads/files/Insurance-Crime-Bureau-2024-Annual-Report.pdf accessed 6 October 2026

IMC 2024 https://www.mas.gov.sg/-/media/mas-media-library/news/media-releases/2024/imc-report.pdf
Inter-Ministerial Committee 2024 *Inter-Ministerial Committee on Anti-Money Laundering* https://www.mas.gov.sg/-/media/mas-media-library/news/media-releases/2024/imc-report.pdf accessed 16 October 2025

IR 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/Guidance-Note-Processing-Special-PersonalInformation-20210628-004.pdf
Information Regulator 2021 *Guidance Note on Processing of Special Personal Information* https://inforegulator.org.za/wp-content/uploads/2020/07/Guidance-Note-Processing-Special-PersonalInformation-20210628-004.pdf accessed 16 October 2025

IR 2025 https://inforegulator.org.za/about/
Information Regulator 2025 *Welcome to the Official Website of the Information Regulator of South Africa* https://inforegulator.org.za/about/ accessed 27 June 2025

Kazlauskas 2023 https://amlyze.com/sars-suspicious-or-defensive-reports/
Kazlauskas E 2023 *SAR: Suspicious, or Defensive Report?* https://amlyze.com/sars-suspicious-or-defensive-reports/ accessed 12 October 2025

La Trobe University 2025 https://www.latrobe.edu.au/news/announcements/2025/lowering-global-barriers-to-financial-inclusion
La Trobe University 2025 *Lowering Global Barriers to Financial Inclusion* https://www.latrobe.edu.au/news/announcements/2025/lowering-global-barriers-to-financial-inclusion accessed 7 September 2026

Libera 2025 https://businesstech.co.za/news/lifestyle/831182/new-crime-tactic-in-south-africa-thats-so-bad-other-countries-are-warning-their-citizens-about-it/
Libera M 2025 *New Crime Tactic in South Africa That's so Bad Other Countries are Warning their Citizens About It* https://businesstech.co.za/news/lifestyle/831182/new-crime-tactic-in-south-africa-thats-so-bad-other-countries-are-warning-their-citizens-about-it/ accessed 10 November 2025

Liive 2021 https://investinestonia.com/estonian-fintech-salv-gives-banks-secure-information-exchange/
Liive R 2021 *Estonian FinTech Salv Gives Banks Secure Information Exchange* https://investinestonia.com/estonian-fintech-salv-gives-banks-secure-information-exchange/ accessed 8 November 2025

Management Solutions 2023 https://www.managementsolutions.com/sites/default/files/minisite/static/7805cb71-d48b-407e-9c40-9353639337c7/fincrime/pdf/financial-crime-en.pdf
Management Solutions 2023 *Financial Crime: Challenges and Trends in the Digital Era* https://www.managementsolutions.com/sites/default/files/minisite/static/7805cb71-d48b-407e-9c40-9353639337c7/fincrime/pdf/financial-crime-en.pdf accessed 6 July 2025

MAS 2021 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf
Monetary Authority of Singapore 2021 *FI-FI Information-Sharing Platform for AML/CFT* https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf accessed 28 June 2025

MAS 2024 https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform
Monetary Authority of Singapore 2024 *MAS Launches COSMIC Platform to Strengthen the Financial System's Defence Against Money Laundering and Terrorism Financing* https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform accessed 16 October 2025

MAS 2025 https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic
Monetary Authority of Singapore 2025 *COSMIC* https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic accessed 28 June 2025

Maxwell 2022 https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf
Maxwell N 2022 *A Survey and Policy Discussion Paper: Lessons in Private-Private Financial Information Sharing to Detect and Disrupt Crime* https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf accessed 28 June 2025

Maxwell 2025 https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf
Maxwell N 2025 *Future of Financial Information Sharing (FFIS) Policy Discussion Paper: A New Era of Private Sector Collaboration to Fight Economic Crime* https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_a_new_era_of_private_sector_collaboration_to_detect_economic_crime_-_policy_discussion_paper_-_march_2025_-_final.pdf accessed 28 June 2025

Moonstone Information Refinery 2023 https://www.moonstone.co.za/draft-amendments-on-information-sharing-between-accountable-institutions-published/
Moonstone Information Refinery 2023 *Draft Amendments on Information-Sharing Between Accountable Institutions Published* https://www.moonstone.co.za/draft-amendments-on-information-sharing-between-accountable-institutions-published/ accessed 25 June 2025

Mvelase 2025 https://www.businesslive.co.za/bd/opinion/2025-07-31-thokozani-mvelase-cybercrime-is-a-state-of-emergency-in-sa/
Mvelase T 2025 *Thokozani Mvelase: Cybercrime is a State of Emergency in SA* https://www.businesslive.co.za/bd/opinion/2025-07-31-thokozani-mvelase-cybercrime-is-a-state-of-emergency-in-sa/ accessed 10 August 2025

Nalog.NL 2024 https://www.nalog.nl/en/news/2024/08/06/svorachivaetsya-programma-proverki-bankovskix-tranzakcij-tmnl/
Nalog.NL 2024 *The Bank Transaction Verification Program is Being Shut Down (TMNL)* https://www.nalog.nl/en/news/2024/08/06/svorachivaetsya-

programma-proverki-bankovskix-tranzakcij-tmnl/ accessed 8 November 2025

National Treasury 2023 https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf
National Treasury 2023 *Financial Intelligence Centre Act, 2001: Draft Amendments to Money Laundering and Terrorist Financing Control Regulations* https://www.treasury.gov.za/Legislation/Regulations/Draft%20Regulations%20-%20Sharing%20of%20information%20between%20accountable%20institutions.pdf accessed 24 June 2025

PMG 2022 https://pmg.org.za/committee-meeting/35924/
Parliamentary Monitoring Group 2022 *General Laws Amendment Bill (Anti-Money Laundering and Combating Terrorism Financing) Bill: National Treasury Briefing* https://pmg.org.za/committee-meeting/35924/ accessed 30 October 2025

PMG 2023 https://pmg.org.za/call-for-comment/1362/
Parliamentary Monitoring Group 2023 *Draft Amendments to Money Laundering and Terrorist Financing Control Regulations* https://pmg.org.za/call-for-comment/1362/ accessed 27 September 2025

Rene and Lambert-Porter 2025 https://www.ropesgray.com/en/insights/alerts/2020/12/transaction-monitoring-netherlands-a-novel-solution-to-the-banking-industrys-aml-puzzle
Rene A and Lambert-Porter S 2025 *Transaction Monitoring Netherlands: A Novel Solution to the Banking Industry's AML Puzzle?* https://www.ropesgray.com/en/insights/alerts/2020/12/transaction-monitoring-netherlands-a-novel-solution-to-the-banking-industrys-aml-puzzle accessed 16 October 2025

Rose 2019 https://www.edb.gov.hk/attachment/en/curriculum-development/kla/eng-edu/professional-development-programmes/1920/LiE_Comparative_Analysis_20200337.pdf
Rose KA 2019 *Personal Development Programme Literature in English 2019/2020 EDB: 'Writing a Strong Comparative Analysis'* https://www.edb.gov.hk/attachment/en/curriculum-development/kla/eng-edu/professional-development-programmes/1920/LiE_Comparative_Analysis_20200337.pdf accessed 26 May 2025

SABRIC 2025 https://www.sabric.co.za/
South African Banking Risk Information Centre 2025 *We are SABRIC* https://www.sabric.co.za/ accessed 27 September 2025

SABRIC 2025 https://www.sabric.co.za/about-sabric/
South African Banking Risk Information Centre 2025 *About Us* https://www.sabric.co.za/about-sabric/ accessed 27 September 2025

SABRIC 2025 https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf
South African Banking Risk Information Centre 2025 *Annual Crime Statistics 2024* https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf accessed 27 September 2025

SAFPS 2025 https://www.safps.org.za/Home/About
South African Fraud Prevention Services 2025 *About Us* https://www.safps.org.za/Home/About accessed 27 July 2025

SAFPS 2025 https://www.safps.org.za/Home/Article_SAFPS_Annual_Report_2024
South African Fraud Prevention Services 2025 *SAFPS 2024 Annual Report* https://www.safps.org.za/Home/Article_SAFPS_Annual_Report_2024 accessed 9 August 2025

SAFPS 2025 https://www.safps.org.za/Home/OurPartners
South African Fraud Prevention Services 2025 *Business and Corporate Members* https://www.safps.org.za/Home/OurPartners accessed 25 September 2025

SAFPS 2025 https://www.safps.org.za/#:~:text=MAKING%20A%20DIFFERENCE,as%20possible%20expansion%20into%20Africa
South African Fraud Prevention Services 2025 *SAFPS Assists in Preventing Fraud as a Result of Identity Theft and Impersonation to Protect You from the Associated Financial Impacts* https://www.safps.org.za/#:~:text=MAKING%20A%20DIFFERENCE,as%20possible%20expansion%20into%20Africa accessed 25 September 2025

Salv 2022 https://salv.com/uploads/AML-Bridge-Estonia.pdf
Salv 2022 *AML Bridge – Building the New Standard in AML/CTF: A Demonstration of FinCrime Intelligence Sharing – Findings and Figures from the AML Bridge Estonia Pilot* https://salv.com/uploads/AML-Bridge-Estonia.pdf accessed 28 June 2025

SAPS 2021 https://www.saps.gov.za/resource_centre/paia/public_manual_popia_2021.pdf
South African Police Service 2021 *Protection of Personal Information Manual of the South African Police Service* https://www.saps.gov.za/resource_centre/paia/public_manual_popia_2021.pdf accessed 16 October 2025

Secretariat 2025 https://secretariat-intl.com/wp-content/uploads/2025/04/Secretariat-Global-Financial-and-Economic-Crime-Outlook-2025.pdf
Secretariat 2025 *Global Financial and Economic Crime Outlook 2025: Introducing the Secretariat Economic Crime Index* https://secretariat-intl.com/wp-content/uploads/2025/04/Secretariat-Global-Financial-and-Economic-Crime-Outlook-2025.pdf accessed 6 July 2025

Singapore Statutes Online 2023 https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628
Singapore Statutes Online 2023 *Financial Services and Markets (Amendment) Act 2023* https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628 accessed 12 November 2025

Tan 2023 https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023
Tan A 2023 *"Financial Services and Markets (Amendment) Bill" – Second Reading Speech by Mr Alvin Tan, Minister of State, Ministry of Culture, Community and Youth and Ministry of Trade and Industry, and Board Member of MAS, on Behalf of Mr Tharman Shanmugaratnam, Senior Minister and Minister-in-charge of the Monetary Authority of Singapore, on 9 May 2023* https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023 accessed 28 June 2025

TMNL 2022 https://tmnl.nl/app/uploads/2022/10/TMNL-Legislaton-EN.pdf
Transaction Monitoring Netherlands 2022 *Legislation* https://tmnl.nl/app/uploads/2022/10/TMNL-Legislaton-EN.pdf accessed 28 June 2025

TMNL 2024 https://tmnl.nl/en/article/transaction-monitoring-netherlands-adapts-its-working-method-to-new-european-legislation/
Transaction Monitoring Netherlands 2024 *Transaction Monitoring Netherlands Adapts Its Working Method to New European Legislation* https://tmnl.nl/en/article/transaction-monitoring-netherlands-adapts-its-working-method-to-new-european-legislation/ accessed 28 June 2025

Transparency International 2024 https://images.transparencycdn.org/images/CPI2024_Report_Eng1.pdf
Transparency International 2024 *Corruption Perceptions Index 2024* https://images.transparencycdn.org/images/CPI2024_Report_Eng1.pdf accessed 7 September 2026

UK Finance 2018 https://www.parliament.uk/globalassets/documents/commons-committees/treasury/Written_Evidence/ecr0064.pdf
UK Finance 2018 *Executive Summary* https://www.parliament.uk/globalassets/documents/commons-committees/treasury/Written_Evidence/ecr0064.pdf accessed 24 October 2025

Walk 1998 https://cbs.umn.edu/sites/cbs.umn.edu/files/migrated-files/downloads/Compcontrastharvard.pdf
Walk K 1998 *How to Write a Comparative Analysis* https://cbs.umn.edu/sites/cbs.umn.edu/files/migrated-files/downloads/Compcontrastharvard.pdf accessed 26 July 2025

Wannenwetsch 2023 https://baselgovernance.org/news/partnering-against-money-laundering-and-corruption-south-africa-and-subregion
Wannenwetsch S 2023 *Partnering Against Money Laundering and Corruption in South Africa and the Subregion* https://baselgovernance.org/news/partnering-against-money-laundering-and-corruption-south-africa-and-subregion accessed 25 September 2025

Yuklea 2025 https://www.feedzai.com/blog/aml-roi/
Yuklea K 2025 *Turning Compliance into Profit: How AML Solutions Deliver ROI* https://www.feedzai.com/blog/aml-roi/ accessed 7 October 2025

List of Abbreviations

AI	accountable institution
AML	anti-money laundering
AML/CTF/PF	Anti-Money Laundering, Counter-Terrorism Financing, and Proliferation Financing
COMRiC	Communications Risk Information Centre
COSMIC	Collaborative Sharing of ML/TF Information and Cases
DoJCD	Department of Justice and Constitutional Development
DPP	data protection and privacy
EU	European Union
FATF	Financial Action Task Force

FAST	fraud attacks and scam transactions
FI	financial institution
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act 38 of 2001
FinCEN	Financial Crime Enforcement Network of the USA
FIU	Financial Intelligence Unit
FSM Act	Financial Services and Markets Act 18 of 2022
GDPR	General Data Protection Regulation
ICB	Insurance Crime Bureau
ID	identification document
IR	Information Regulator
MAS	Monetary Authority of Singapore
ML	money laundering
ML/TF	money laundering and terrorism financing
ML/TF/PF	money laundering, terrorism financing, and proliferation financing
NPO	non-profit organisation
P2P	private-private information sharing
PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 56 of 2001, USA
PDPA	Personal Data Protection Act 26 of 2012
PELJ	Potchefstroom Electronic Law Journal
PF	proliferation financing
PMG	Parliamentary Monitoring Group
POCA	Prevention of Organised Crime Act 121 of 1998
POCDATARA	Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004
POPIA	Protection of Personal Information Act 4 of 2013
PRECCA	Prevention and Combating of Corrupt Activities Act 12 of 2004
SA	South African
SABRIC	South African Banking Risk Information Centre
SAIA	South African Insurance Association
SAFPS	South African Fraud Prevention Services
SAPS	South African Police Services

SAR	Suspicious Activity Report
SARB	South African Reserve Bank
SECI	Secretariat Economic Crime Index
SISS	Secure Information Sharing System
STR	suspicious transaction report
TF	terrorism financing
TMNL	Transactie Monitoring Nederland / Transaction Monitoring Netherlands
UNCAC	United Nations Convention Against Corruption (2003)
US/USA	United States of America