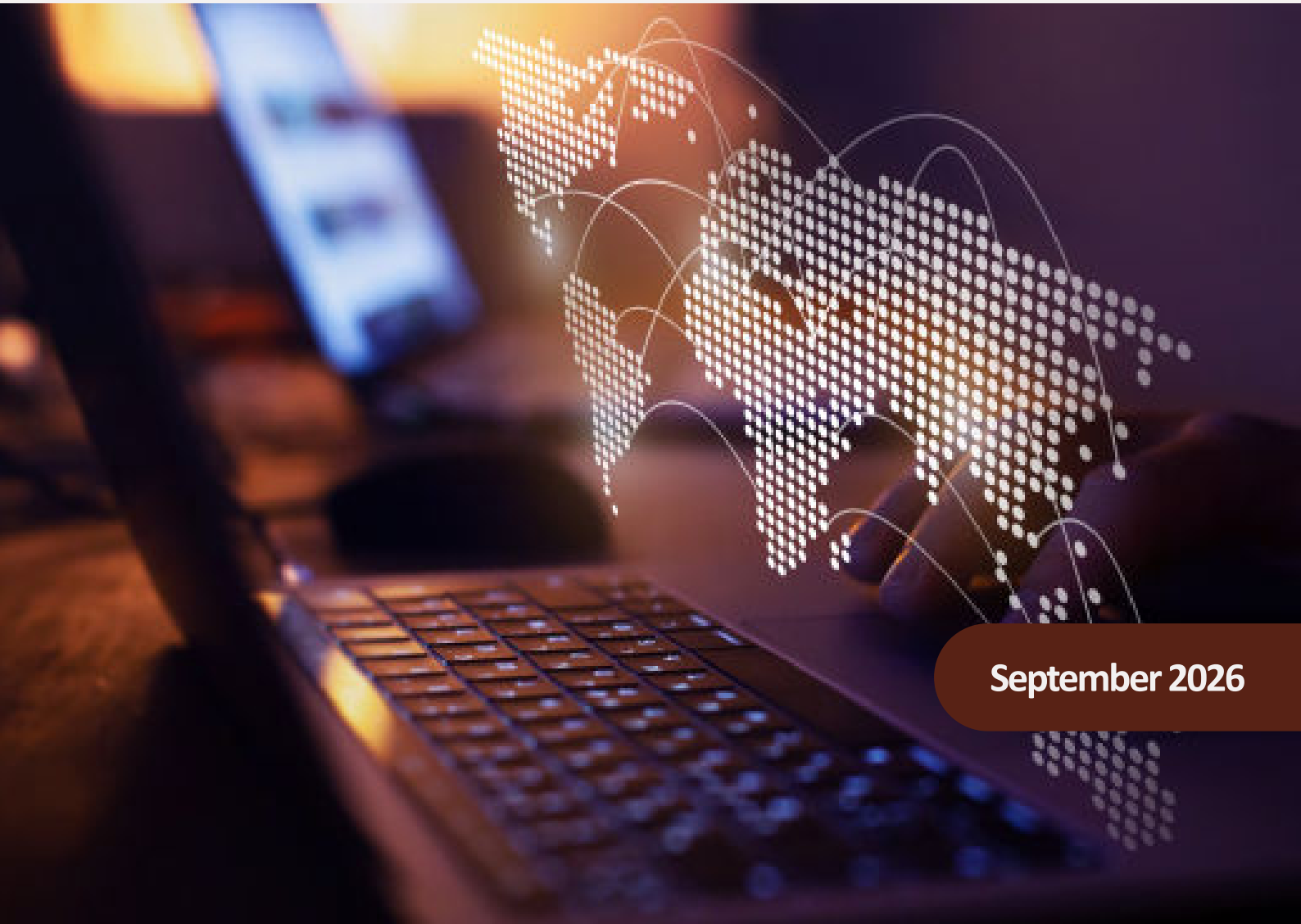
FATF Report

Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers



September 2026

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops an policies to protect the global financial system against money laundering, terrorist financing and the proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereign territory, to the delimitation of international frontiers and boundaries and to the name of any territory, ci

Citing reference:

FATF (2026), *Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers, Paris, France*, *https://www.fatf-gafi.org/en/publications/Methodsandtrends/pml-underground-banking-hawala-hossps*

Photo credits cover photo ©Shutterstock

Table of contents

1. Acronyms

Acronym	Description
AML	Anti-money laundering
BMPE	Black market peso exchange
BO	Beneficial ownership
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CULINT	Cultural intelligence
DNFBP	Designated non-financial businesses and professions
EU	European Union
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial intelligence unit
FX	Foreign exchange
HOSSP	Hawala and other similar service provider
ICN	International controller network
KYC	Know your customer
LEA	Law enforcement authority
ML	Money laundering
MVTS	Money or value transfer service
MLA	Mutual legal assistance
MSB	Money service business
NPO	Non-profit organisation
NRA	National risk assessment
OSINT	Open-source intelligence
PF	Proliferation financing
PML	Professional money laundering
PPP	Public-private partnership
PSP	Payment service provider
SAR	Suspicious activity report
STR	Suspicious transaction report
TBML	Trade-based money laundering
TBTF	Trade-based terrorist financing
TF	Terrorist financing
VA	Virtual asset
VASP	Virtual asset service provider
vIBAN	Virtual international bank account number

2. Executive summary

1. Underground banking, hawala, and other similar service providers (HOSSPs) are long-standing value-transfer and other financial service systems whose operational practices vary by region and level of sophistication. They function as informal, decentralised networks that are distinct from, though sometimes interconnected with, the formal financial sector. Their defining feature is the transfer of value without the physical cross-border movement of funds, with obligations settled through compensation mechanisms including trade transactions, cash pooling, formal financial channels, or alternative asset movements. While underground banking and HOSSPs may operate outside or alongside the regulated financial system and may serve legitimate remittance and value-transfer needs, they may also be exploited by criminal actors, including professional money launderers, to facilitate illicit financial activity.

2. The FATF has long recognised the money laundering (ML) and terrorist financing (TF) risks associated with underground banking and HOSSPs, including their role as a significant tool used by professional money laundering (PML) networks. Since the FATF's 2013 report, *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, the underlying risk factors have remained relevant, including anonymity and limited transparency, speed, convenience, accessibility, low cost, profitability and reliability. At the same time, the use of underground banking and HOSSPs for PML has continued to evolve in response to developments in the criminal economy and rapid technological change, including encrypted communications, fintech, anonymity-enhancing tools, and the growing use of virtual assets (VAs).

3. Against this background, this report examines the roles, methods and typologies of underground banking and HOSSPs in PML, as well as the capabilities and responses of competent authorities to these phenomena.

Evidence base

4. The report was prepared by a project team of 22 FATF Members, 7 members of FATF-Style Regional Bodies, and 3 FATF Observers. Forty-six jurisdictions responded to two questionnaires circulated in September 2025 and February 2026, and expert practitioners provided additional insights during a dedicated session at the Joint Experts Meeting in November 2025. These contributions form the evidence base for the report.

Key findings

5. The report finds that the use of underground banking and HOSSPs is not inherently criminal and may be used to move both legitimate and illicit funds. However, in most countries, the provision of underground banking or unregistered HOSSP services is generally a criminal offence, and is in contravention to the FATF Standards which recommend that countries require these entities to be licensed or registered to provide such services. Criminal misuse of HOSSPs and underground banking more generally for PML is a **widespread global phenomenon** that may occur regardless of the legal status of these systems. Such misuse is **particularly prominent along certain corridors and in specific regions, often in connection with strong remittance flows, dense trade links, long-standing diaspora communities, and low levels of formal financial intermediation**. The report also

finds that there is a growing convergence between traditional informal transfer networks and increasingly sophisticated and professionalised ML structures.

6. The report shows that underground banking- and HOSSP-related **PML is no longer exclusively associated with traditional cash-intensive crimes** such as drug trafficking or smuggling but increasingly serves as an ML infrastructure for a broader spectrum of criminal economies, including **fraud, cyber-enabled crime, corruption, tax evasion, TF, undeclared work, illegal gaming and gambling, and transnational organised crime** generating proceeds from diverse activities.

7. A central finding of the report is an updated typology of underground banking and HOSSP settlement modalities reflecting current practices and technological developments.

8. One of the most significant developments identified in the report is the **digital transformation of underground banking and HOSSP activity**, including the use of digital technologies to facilitate the co-ordination, execution, settlement, or concealment of informal value transfer, including for PML. Sometimes referred to as "digital hawala", this transformation does not constitute a single, uniform phenomenon. Rather, it covers a spectrum of practices, ranging from the digitalisation of communications to the integration of VAs and electronic payment technologies into settlement mechanisms. The report finds that this digitalisation can accelerate customer-operator interaction and cross-border settlement, increase opacity and evidential challenges, expand layering opportunities, and strengthen the geographic reach and resilience of underground banking- and HOSSP-based PML schemes.

9. The report also identifies **several broader global trends**. These include:

(i) diversification of client profiles;

(ii) increasing professionalisation of these schemes, reflected in more structured and service-oriented ML infrastructures, specialised roles, standardised processes, and the growing use of professional intermediaries and enablers; and

(iii) deep integration with the formal financial sector, as PML actors increasingly combine informal value-transfer mechanisms with licit financial infrastructures in order to exploit regulatory asymmetries and supervisory blind spots. In this context, formal financial accounts, fintech platforms, payment service providers, virtual IBANs, prepaid cards, and VA wallets are increasingly used as entry and exit points in ML cycles.

10. **Regional typologies are also identified**, such as the integration of underground banking and HOSSPs with mobile money systems in Africa and Asia, and hybrid settlement models involving VAs and precious metals and stones in the Middle East. The report also highlights typologies associated with high-capacity transnational PML networks rooted in geographic and demographic ties. In addition, the report underscores the emergence of regional hub structures, whereby certain jurisdictions or geographic clusters play recurrent roles in the cross-border settlement, clearing or absorption of illicit value within transnational informal value-transfer networks.

Risk mitigation challenges

11. The report highlights a number of challenges for jurisdictions in regulating, detecting, investigating and prosecuting the misuse of underground banking and HOSSPs for PML. These include:

(i) fragmented terminology and definitions;

(ii) persistent knowledge gaps resulting from the limited visibility jurisdictions have over how these systems operate; and

(iii) regulatory asymmetries, both across borders and within jurisdictions, which create arbitrage opportunities exploited by PML networks.

12. Jurisdictions may also face difficulties in distinguishing legitimate activity from criminal misuse and, in some cases, de-risking pressures or financial incentives may divert legitimate remittance users and some formal money value transfer services (MVTS) providers into informal channels.

13. Operational challenges remain significant, including the fragmented and resilient structure of PML networks, limited standardised intelligence and red flags, difficulties in monitoring digital components, constraints affecting traditional investigative approaches, challenges in international co-operation and evidential difficulties in establishing criminal intent and tracing complete ML chains.

Good practices in detecting, investigating, prosecuting, and disrupting PML operations

14. To address these challenges, Section 3 of the report sets out good practices to support practitioners in financial intelligence units (FIUs), law enforcement authorities (LEAs), prosecution services, and supervisory bodies in detecting, investigating, prosecuting, and disrupting PML operations facilitated by underground banking and HOSSPs. The report stresses that prevention and enforcement must work in parallel.

15. Good practices include:

(i) establishing a clear legal and regulatory environment;

(ii) adopting a system-wide, holistic approach to disrupting PML chains rather than a purely case-by-case approach;

(iii) creating dedicated domestic co-ordination mechanisms across competent authorities and, where relevant, with private-sector partners;

(iv) focusing on the intersections between underground banking and HOSSPs and the formal financial system;

(v) leveraging advanced supervisory and investigative techniques and technologies, subject to legal and practical constraints;

(vi) engaging affected communities and sectors to strengthen detection and compliance; and

(vii) deepening international co-operation on underground banking- and HOSSP-based PML schemes.

16. In particular, strengthening detection capabilities – including beyond traditional tools – emerges as a priority area to improve the identification, analysis and reporting of suspicious activity.

17. The report also underscores the importance of combining targeted enforcement against the criminal exploitation of underground banking and HOSSPs with proportionate financial inclusion measures, in order to reduce reliance on illegal informal value-transfer channels.

18. This report should be considered an awareness-raising tool for both public- and private-sector stakeholders. More specifically, as the features and conditions that make underground banking and HOSSPs attractive to professional money launderers are likely to persist, this report calls on jurisdictions to strengthen their regulatory and operational responses, including through effective implementation of the FATF Recommendations (including Recommendations 3, 5 and 14) and improved effectiveness under Immediate Outcomes 3 and 7.

3. Introduction

19. Since the early 2000s, the FATF has recognised the ML/TF risks associated with underground banking and hawala and other similar service providers (HOSSPs). Notably:

(i) In 2013, the FATF published the report *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*[1], finding that while underground banking systems and HOSSPs may serve legitimate purposes, they remain vulnerable to ML/TF.

(ii) In 2018, the FATF published the report *Professional Money Laundering*[2], which documented large-scale global PML operations involving underground banking and HOSSPs.

20. Also, half of FATF jurisdictions and nearly 30% of Global Network jurisdictions assessed during the fourth round of mutual evaluations (2014–2024) identified HOSSPs as high-risk for ML and TF.

21. Since then, the risk landscape has continued to evolve, compounded by significant developments, including rapid technological innovation, anonymity-enhancing technologies, and the widespread use of encrypted communications.

3.1. Scope of the project

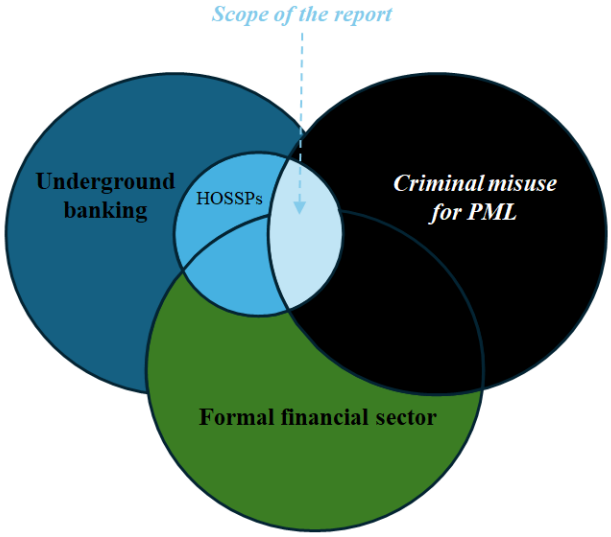
22. This project examines the roles of underground banking and HOSSPs in professional money laundering (PML) typologies, as well as the responses of competent authorities to these trends. The analysis focuses on the intersection between a specific threat—criminal actors specialising in the provision of PML services—and the vulnerabilities that certain HOSSPs and underground banking models present (see Infographic 1).

[1] FATF (2013), *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

[2] FATF (2018), *Professional Money Laundering*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf

Infographic 1. Criminal exploitation of underground banking, HOSSPs, and the formal sector

This infographic illustrates the intersections between underground banking, HOSSPs and the formal financial sector. All three sectors may be exploited by professional money launderers to conduct PML activities. However, this report focuses on the criminal misuse of those intersections.



3.1.1. Key terminology

23. The key terminology applicable to this report is defined as follows.

Professional money laundering

24. Consistent with the FATF's 2018 report on *Professional Money Laundering*[3], this study characterises PML as the laundering of proceeds by individuals, organisations, or networks not involved in the commission of the predicate offence.

25. PML is a subset of third-party money laundering, as opposed to self-laundering, and refers to individuals, organisations or networks providing ML services to criminals in exchange for a commission, fee, or other profit. Such actors may operate as or include professional service providers, whether regulated or unregulated.

26. Europol refers to this model as "money laundering as a service", highlighting the systematic outsourcing of ML functions to specialised facilitators and the emergence of PML as a commercialised business model.

27. Professional money launderers typically establish and maintain enduring ML infrastructure, including shell companies and other legal persons or arrangements, and rely on facilitators and multiple layers of intermediaries to distance themselves from predicate offences and conceal their role. They may

[3] FATF (2018), *Professional Money Laundering*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf

themselves obtain financial or regulatory licenses to enhance their access to the financial system.

28. PML operations are often cross-border in nature, even where predicate funds are generated domestically, and may involve the receipt and storage of proceeds for a defined or indefinite period prior to onward movement or integration. They range from highly structured and sophisticated schemes—using mechanisms such as international wire transfers, offshore and onshore accounts, and complex legal arrangements—to relatively simple methods, including cash-based or loan-back constructions involving only a limited number of actors.

29. While professional money launderers may exploit the full spectrum of ML techniques, this FATF project focuses specifically on how they misuse HOSSPs and other underground banking models.

Underground banking

30. Consistent with the FATF's functional approach, this study defines underground banking as informal financial arrangements that operate both outside and through the regulated financial system to enable the transfer, settlement, or storage of value through networks of intermediaries. Such arrangements may rely on value-transfer mechanisms—hence their intersection with the realm of HOSSPs—but may also employ a broader range of mechanisms.

31. The use of underground banking systems is not inherently criminal, for example where legitimate actors use such services to transfer licit funds. However, the provision of unlicensed underground banking services is generally a criminal offence in most countries and is inherently non-compliant with the FATF Standards, as it constitutes the provision of unregulated financial services. At the same time, the legal treatment of these services varies across jurisdictions, and they may be legal where the host jurisdiction is not compliant with certain aspects of the FATF Standards. Regardless of their legal status, such systems present elevated ML and TF risks due to limited transparency, reliance on informal settlement mechanisms, and, in some cases, operation outside licensing, registration, or supervisory frameworks.

32. Underground banking manifests differently across regions. Selected examples illustrate the breadth of arrangements captured by this concept, beyond HOSSP arrangements. For instance, in East and Southeast Asia, UNODC has documented a digitised and casino-linked manifestation of underground banking (distinct from HOSSP-based models), in which casinos, junkets, online gambling platforms, and VA exchanges form part of underground banking and ML infrastructure[4].

33. Related concepts used by several jurisdictions include "parallel financial system" and "shadow banking", which capture how informal mechanisms complement or replace formal channels in PML operations. However, the notion of a 'parallel financial system' may understate the extent to which such mechanisms intersect with, and rely upon, elements of the formal financial sector (see subsection 7.1.3.).

[4] UNODC (2024), *Casinos and cryptocurrency: major drivers of money laundering, underground banking, and cyberfraud in East and Southeast Asia*, UNODC Regional Office for Southeast Asia and the Pacific, Bangkok, Thailand, https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html?

Hawala and other similar service providers

34. For the purposes of this report, and in alignment with the 2013 FATF report on *The Role of Hawala and Other Similar Service Providers in ML/TF*[5], HOSSPs are defined as a subset of MVTS that arrange the transfer and receipt of funds or equivalent value, and settle through various mechanisms, often on a net basis over extended periods via trade or cash. When licensed or registered in line with FATF Recommendation 14, HOSSPs are a subset of MVTS within the formal financial sector; when unlicensed or unregistered, HOSSPs are an illegal subset of MVTS within underground banking.

35. As a development since the 2013 report—which noted that HOSSPs were characterised by non-bank settlement—this study shows that contemporary HOSSP networks may also use formal financial channels, including bank accounts, payment service providers (PSPs) or other regulated services, as part of hybrid settlement arrangements or as entry and exit points within broader value-transfer chains.

36. While HOSSPs may operate outside or alongside the regulated financial system, their use is not inherently criminal and may serve legitimate remittance and value-transfer needs. However, they may also be exploited or misused by criminal actors, including professional money launderers, to facilitate illicit financial activity. This report focuses specifically on the misuse of HOSSPs for PML.

37. HOSSPs are often associated with particular geographic regions or ethnic communities and may be referred to using varied terminology that reflects cultural and linguistic contexts. Among jurisdictions responding to the survey, 67% explicitly use the term *hawala*, which appears in all regions and remains the most widely recognised reference term. *Hundi* is widely used in Asia, while other locally used terms include *osusu*, *maraka* and *amana* in West Africa, *chika ginko*, *hui kuan*, *padala*, and *fei qian* in East Asia or *box hand*. Several jurisdictions also referred to 'informal remittance networks', 'informal value-transfer systems' or 'informal fund transfer systems'.

3.2. Objectives

38. The objectives of this report are threefold:

(i) Establishing the current state of play regarding the use of PML through underground banking and HOSSPs, with a view to promoting greater global consistency in terminology and developing a shared evidentiary basis across jurisdictions.

(ii) Outlining and assessing the challenges posed to competent authorities by recent developments in the use of underground banking and HOSSPs for PML.

(iii) Identifying good practices, including practical tools, to assist competent authorities in detecting, investigating, prosecuting, and disrupting PML operations facilitated by underground banking and HOSSPs.

[5] FATF (2013), *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

3.3. Structure of the report

39. Section 1 provides an overview of the context and operating mechanisms underpinning the misuse of underground banking and HOSSPs for PML, including the factors that make these systems vulnerable to such misuse. It places particular emphasis on settlement methods and emerging typologies, highlighting the increasing digitalisation, professionalisation, integration with the formal financial sector, and broader expansion of PML operations involving underground banking and HOSSPs.

40. Section 2 identifies key challenges faced by jurisdictions in addressing the misuse of underground banking and HOSSPs for PML, including persistent knowledge gaps, fragmented definitions, regulatory asymmetries and de-risking effects, and significant operational difficulties in detecting, investigating and prosecuting these networks.

41. Section 3 identifies effective mitigation strategies and good practices for competent authorities—including financial investigation units, law enforcement authorities, prosecutors, and supervisors—to counter the misuse of underground banking and HOSSPs for PML.

3.4. Methodology

42. This project was co-led by Germany and Saudi Arabia and supported by a project team comprising 32 jurisdictions representing all FATF regions and three Observers[6]. The project team applied the following methodology:

(i) A literature review, including FATF publications and work produced by other international organisations —such as UNODC[7] and INTERPOL—as well as by think tanks and jurisdictions.

(ii) Analysis of responses to two questionnaires: the first, launched in September 2025, gathered inputs from 44 jurisdictions[8]; the second, more targeted questionnaire was launched in February 2026 and enabled to gather further contributions from 11 jurisdictions[9]. Both questionnaires enabled the collection of risk assessments, case studies, and examples of good practices related to countering the use of underground banking and HOSSPs for PML.

(iii) Expert consultations and discussions held throughout the project, including during project team meetings, October 2025 and February 2026 RTMG

[6] The project team comprised experts from 32 jurisdictions, including 22 FATF Members: Australia, Belgium, Canada, China, Estonia, France, Germany (co-lead), India, Israel, Luxembourg, Mexico, Netherlands, New Zealand, Portugal, Saudi Arabia (co-lead), Singapore, South Africa, Spain, Switzerland, Türkiye, United Kingdom, United States; 7 FSRB Members: Azerbaijan, Bangladesh, Burkina Faso, Kyrgyzstan, Montserrat, Nigeria, Pakistan; and 3 Observers: Europol, INTERPOL, and UNODC.

[7] UNODC (2023), *The Hawala System: Its Operations and Misuse by Opiate Traffickers and Migrant Smugglers*, UNODC, Vienna, https://www.unodc.org/documents/data-and-analysis/AOTP/Hawala_Digital.pdf

[8] Australia, Azerbaijan, Bangladesh, Belgium, Burkina Faso, Canada, China, Comoros, Côte d'Ivoire, Denmark, Djibouti, Egypt, Estonia, Europol, France, Gambia, Germany, Greece, Hong Kong China, India, Indonesia, Iraq, Italy, Japan, Luxembourg, Mexico, Malaysia, Montserrat, Netherlands, North Macedonia, New Zealand, Nigeria, Oman, Pakistan, Portugal, Russian Federation, Saudi Arabia, South Africa, Spain, Sweden, Switzerland, Togo, Türkiye, and the United Kingdom.

[9] Argentina, Australia, Belgium, Canada, China, France, Germany, Ireland, Japan, Luxembourg, and Portugal.

meetings, and the Joint Experts Meeting in Accra, Ghana, from 4 to 6 November 2025.

(iv) Reviews of the first and second draft reports by the Global Network in February and April 2026, respectively.

Section 1 – State of play of the use of underground banking and HOSSPs for professional money laundering

4. Underground banking and HOSSPs as they operate irrespective of PML misuse

43. Nearly 90% of jurisdictions responding to the survey reported the presence of underground banking systems and HOSSPs within their territories.

44. Underground banking and HOSSPs usually operate as informal and decentralised, value-transfer networks, that are distinct from, but may intersect with, the formal financial sector. Their defining feature is that value is transferred without the physical movement of funds across borders. Instead, counterpart operators in different jurisdictions settle obligations through internal book-entries and subsequent compensation, which may involve trade transactions, cash pooling, or alternative asset movements. Although operational practices vary by region and level of sophistication, the core architecture remains broadly consistent worldwide (see Infographic 2):

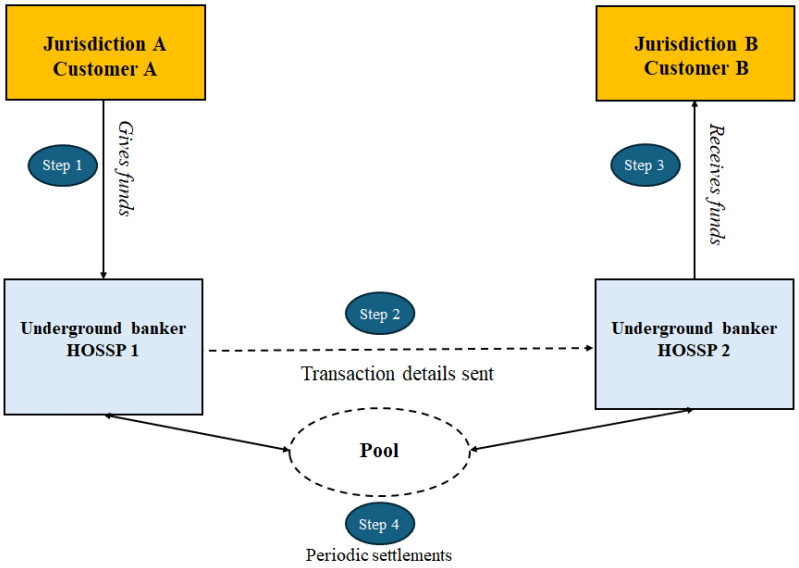
(i) Step 1: Customer A wishes to transfer funds to Customer B located in another jurisdiction. Customer A provides local currency to HOSSP 1 in Jurisdiction A.

(ii) Step 2: HOSSP 1 transmits transaction details to HOSSP 2 in Jurisdiction B through informal communication channels (e.g., telephone, messaging applications, encrypted platforms, email or community intermediaries).

(iii) Step 3: HOSSP 2 pays the equivalent value to Customer B (typically immediately and in local currency) using a local cash pool or third-party business account. No physical or electronic movement of monies occurs at this stage. Both HOSSPs record their obligations in internal ledgers.

(iv) Step 4: HOSSPs later settle outstanding balances between themselves, taking into account the accumulated transactions since the previous reconciliation. Settlement may occur through a variety of ways. A classification of settlement methods is presented in subsection 1.7. below.

Infographic 2. General operating model of underground banking and HOSSPs



45. The key components found across underground banking and HOSSP networks typically include:

(i) **Underground bankers/Hawaladars**: Network brokers controlling cash pools and ledgers, frequently operating from legitimate ancillary businesses (e.g., travel agencies, money exchange shops, import/export firms, wholesalers).

(ii) **Pools**: Reserves held by brokers to ensure immediate payment capacity, sourced from commercial flows, legitimate remittances or criminal proceeds.

(iii) **Customers**: Individuals or businesses seeking fast, discreet or low-cost transfers, including both legitimate remittance users and criminal actors.

(iv) **Remuneration**: Operators are predominantly remunerated through commission-based fees, typically ranging from approximately 0.5% to 5%, although these may vary significantly depending on circumstances, particularly in higher-risk or high-volume ML arrangements. Fee levels are explicitly risk-based, with transfers involving funds suspected to originate from criminal activity attracting higher charges to reflect increased detection risk, criminal liability, and potential prosecution. Remuneration is further influenced by destination-specific and operational factors, including the use of remote or conflict-affected regions, politically or economically unstable environments, complex cross-border routes, transaction size, payout currency, urgency, and the nature of the customer relationship, with smaller transactions often subject to disproportionately higher percentage fees. Overall, these features indicate that underground bankers and HOSSPs engaged in PML operate as systematically remunerated professional service providers, using flexible, opaque, and risk-based pricing structures that sustain their networks and help conceal illicit profits within ordinary transaction parameters.

(v) **Clearing mechanisms**: Methods used to balance obligations, such as trade-based transactions, cash smuggling, VA transfers or deposits made through mule accounts.

46. Reputation and performance are central to underground banking and HOSSP. Relationships are typically based on repeat business, community visibility, and enforceable consequences for non-performance. Customers select providers based on their reliability, and failure to meet expectations can quickly undermine an operator's standing within the network.

47. In the majority of cases, jurisdictions report that underground banking systems and HOSSPs operate ancillary businesses, most commonly import/export and trading companies, followed by professional service firms (e.g., law or accountancy practices, real estate brokers, other professional enablers), convenience stores, gas stations and small retail outlets, restaurants, bars and nightclubs, formal MVTS providers, precious metals and stones traders, luxury goods retailers, travel agencies, vehicle dealerships, parking facilities and car washes, casinos and gambling establishments, mobile phone shops, currency exchangers, and construction companies.

48. Regarding the profiles of providers and users, most jurisdictions reported an absence of reliable quantitative data. Nonetheless, responses allow for some broad inferences. Predominant provider categories include male, although female operators are increasingly visible in certain jurisdictions. On the user side, principal groups include migrant workers and diaspora families, small and medium traders, and criminals exploiting these systems for tax evasion and ML. Users may be male or female, but women appear more frequently as users than as providers.

49. Across all regions, diaspora and migration emerge as central drivers shaping both demand and supply. Community and ethnicity-based networks form a structural foundation, although providers and users do not necessarily share the same cultural or national background.

5. Role of underground banking and HOSSPs in PML

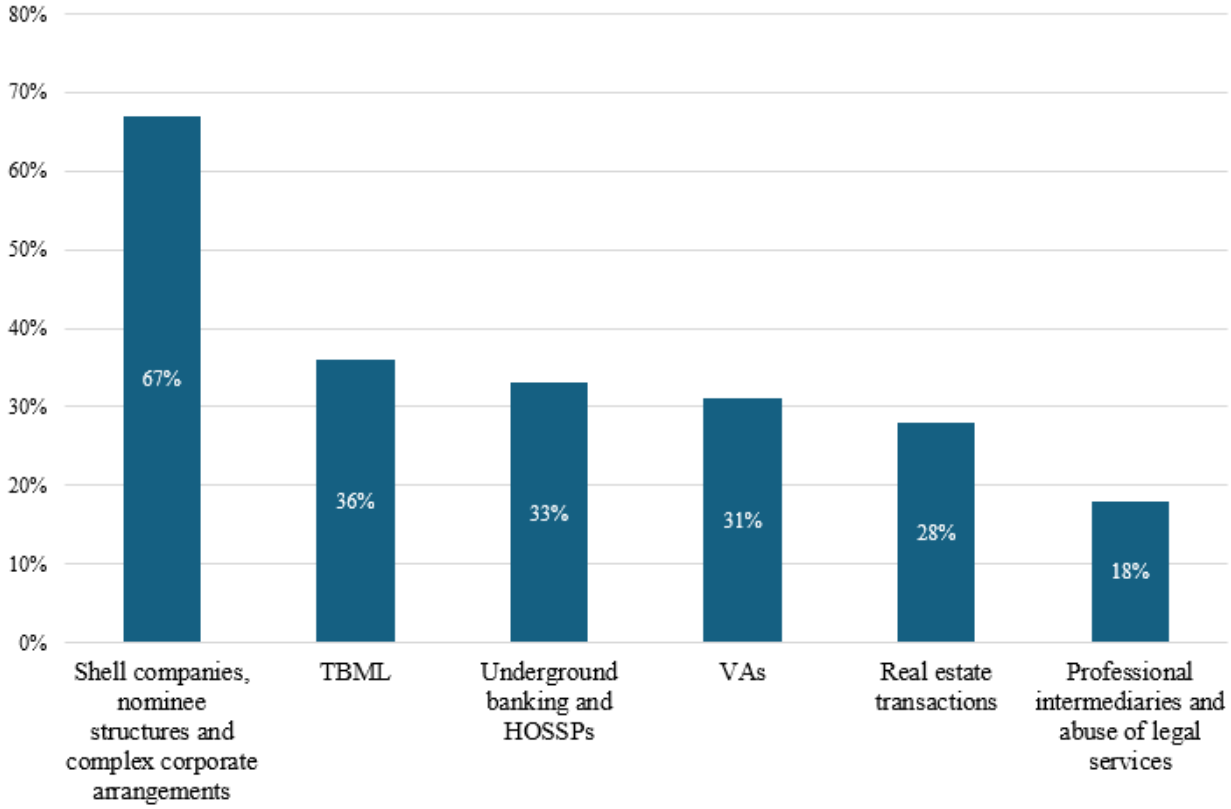
5.1. Prevalence

50. Underground banking networks and HOSSPs present heightened risks of misuse for ML and TF, a concern reflected in the national risk assessments (NRAs) of more than 60% of responding jurisdictions. Consistent with this, more than 80% of jurisdictions identify these systems as among the principal channels and techniques through which PML activities are conducted within their territories (see Infographic 3).

51. At the same time, the survey results do not allow for robust quantitative assessment or reliable comparisons of prevalence across regions. This is largely due to common detection limitations which significantly constrain visibility. Nevertheless, qualitative responses and case studies indicate that such activity is particularly prominent along certain corridors and in specific regions where underground banking networks and HOSSPs are well established, with the use of these systems for PML most frequently reported in Asia, Western Europe, and West Africa.

Infographic 3. Main channels and techniques used for PML

Percentage of jurisdictions responding to the survey identifying each channel or technique:



5.2. Drivers of vulnerability

52. The prevalence of underground banking and HOSSPs in PML activity can be explained not only by a set of intrinsic characteristics that make them particularly suitable for laundering large volumes of illicit funds, but also by external, structural, cultural, and contextual factors that reinforce and compound these vulnerabilities. Across regions, underground banking and HOSSPs appear highly attractive to professional money launderers due to the way these factors interact to enable the discreet, rapid, and cost-efficient movement and laundering of proceeds of crime.

53. These drivers also explain the continued growth and diversification of their client base. Across multiple jurisdictions, transnational organised crime groups remain the primary users of underground banking and HOSSPs for PML. However, the range of high-risk users is expanding to include corrupt officials and politically exposed persons, fraudsters and cybercriminals, terrorist financiers, tax evaders, and wealth-concealers. Client bases increasingly combine users transferring funds of licit origin with those seeking to launder criminal proceeds. In many jurisdictions, underground banking systems knowingly and unknowingly serve both communities seeking financial inclusion and criminal actors exploiting the same channels for concealment and cross-border ML.

54. Respondent jurisdictions consistently identify four main intrinsic drivers underpinning the attractiveness of underground banking and HOSSPs for PML,

suggesting that these systems are particularly well suited to enabling the movement and laundering of high volumes of illicit funds:

(i) **Anonymity and lack of transparency** are among the most frequently cited intrinsic features, reported by more than half of responding jurisdictions. The limited transparency inherent in underground banking and HOSSPs—stemming from the fact that value is transferred without necessarily moving monies themselves—facilitates anonymity for customers as well as for the source, destination, and purpose of funds. The settlement mechanisms on which these systems rely significantly limit traceability, obscure transaction flows, and constrain the ability of competent authorities to reconstruct transfers or determine the origin and ultimate destination of value.

(ii) **Speed, convenience, and accessibility** are also widely cited as key drivers. Underground banking and HOSSP networks can settle transfers across multiple jurisdictions and currencies in short timeframes. These networks offer globally accessible services, including in remote areas or regions where formal financial infrastructure is limited, thereby significantly shortening the interval between the initial placement of funds and their subsequent transfer across jurisdictions. Professional money launderers leverage these characteristics to consolidate, convert, and move illicit proceeds rapidly, facilitating swift layering and distribution while bypassing regulated channels. The ability to reach remote or sensitive areas also allows professional money launderers to extend their services to a broader range of clients.

(iii) **Low cost and enhanced profitability** represent a further intrinsic driver. The low costs associated with underground banking and HOSSPs were repeatedly cited as a key advantage, as informal structures reduce operational expenditures and support competitive pricing compared to licensed money service businesses (MSBs). A key aspect of underground banking and HOSSP's low cost and profitability, particularly where it is misused for PML, is the ability to charge both criminal clients and underground banking or HOSSP clients for the same transaction. This allows professional money launderers to be paid at both ends of the transaction and to charge lower commission fees for ML.

(iv) **Reliability and reputation** further enhance the attractiveness and resilience of underground banking and HOSSPs, with regional specificities shaping how these attributes are established and maintained. In certain jurisdictions, particularly in Asia, West Africa, and other parts of Africa, where underground banking and HOSSPs have long been established and widely practised, cultural embeddedness and community-based reputation play a significant role. These systems rely on social ties, community solidarity, and reputation-based guarantees, providing social legitimacy, accessibility, and confidence for users even in the absence of formal regulatory oversight.

55. In many jurisdictions, multiple overlapping contextual risk layers compound these intrinsic features, creating dominant enabling conditions for the misuse of underground banking and HOSSPs for PML:

(i) **Economic and social factors:** Cash-based or informal economies; large unbanked populations driven by lack of access to formal banking or de-risking practices; cheaper facilitation of remittances via HOSSPs; high remittance

flows and reliance on migrant workers; and high volumes of cross-border trade. In some cases, deep integration into global finance paradoxically sustains informal alternatives for covert or rapid transfers.

(ii) **Geographic factors:** Porous borders and extensive coastlines facilitating informal trade; proximity to high-risk or conflict zones; and the presence of cross-border diaspora corridors.

(iii) **Legal and regulatory factors:** Weaknesses in legislation, supervision, and enforcement, including regulatory inconsistencies and blind spots; restrictions on capital movement, including state capital controls and economic sanctions, combined with reliance on informal remittances; de-risking by financial institutions (FIs) excluding certain sectors or clients; legal constraints that unintentionally encourage the use of illicit channels; and, in some cases, strong Anti-Money Laundering / Combating the Financing of Terrorism (AML/CFT) regimes that may push PML activity into informal spaces.

56. These intrinsic and contextual vulnerabilities have, over at least the past two decades, been further exacerbated by developments in the criminal economy, most notably the geographical expansion of organised crime networks involved in drug trafficking and multiple other criminal sectors, including migrant smuggling and arms trafficking, among others. Drug trafficking, in particular, remains one of the dominant predicate offences associated with PML, and its growth has intensified the exploitation of underground banking systems and HOSSPs (see subsection 5.4.).

57. Looking ahead, respondent jurisdictions anticipate that the risk of misuse of underground banking and HOSSPs for PML will continue to increase. This expectation is driven by three converging forces: the persistence of intrinsic features that inherently lend themselves to PML; contextual environments conducive to their continued operation; and the demonstrated ability of these systems to adapt to technological change and successfully embrace digitalisation (see subsections 6.5 and 7.1.1.).

5.3. Distinctive features

58. When underground banking and HOSSPs are misused for PML, additional roles and mechanisms—beyond those described in subsection 4—are frequently observed, including:

(i) **Tokens**: In the context of criminal transfers conducted through underground banking and HOSSPs, tokens are typically used as a simple authentication and control mechanism to ensure that cash is paid out to the intended recipient and to evidence that a handover has occurred. Tokens most commonly take the form of a unique serial number on a banknote. The use of such tokens is a regular feature of criminal cash handovers: the serial number is communicated through the transfer chain and must be produced or matched at the point of collection, thereby providing a basic form of identification and a rudimentary receipt. When seized in a criminal investigation, tokens—and associated records such as ledgers or messaging logs—can be used by prosecutors to demonstrate the operational methodology of criminal underground banking and HOSSP activity.

(ii) **Controllers**: In line with the FATF 2013 report[10], controllers—also referred to in some jurisdictions as 'money brokers' or 'superfacilitators'—are trusted individuals who arrange the collection of criminal proceeds and the delivery of equivalent value to the intended destination. In contemporary PML schemes, this role may extend beyond individual cash handovers to the co-ordination of correspondent brokers, collectors, co-ordinators, transmitters, and other in-country representatives across jurisdictions. Controllers may manage pricing, credit limits, settlement channels, liquidity, and risk controls, and may retain margins linked to liquidity provision, fees, and currency differentials. Other participants may receive fixed or percentage-based commissions according to function and risk exposure. In some jurisdictions, authorities refer to such structures as 'money laundering network controllers' or 'international controller networks (ICNs)'. These networks may make extensive use of underground banking and HOSSPs within broader PML schemes. Identifying controllers and their in-country representatives remains a key success factor for competent authorities seeking to detect, map, and disrupt these networks.

59. When misused for PML, underground banking and HOSSPs typically operate clandestinely, often through outwardly legitimate fronts, and are deliberately concealed from regulators and law enforcement. This concealment is consistently observed across regions.

60. Underground banking- and HOSSP-based PML operations do not function as isolated systems. Approximately 80% of jurisdictions report that such schemes are used in combination with other ML methods, forming hybrid PML pipelines. The most frequently observed combinations involve trade-based money laundering (TBML), shell and front companies, VAs, real estate, luxury goods, and precious metals and stones. These sectors act as entry, settlement, or integration mechanisms, enabling illicit proceeds to circulate between informal networks and the regulated economy.

61. Underground banking and HOSSP services are also frequently embedded within broader criminal service offerings, including the provision of false documentation, advice on ML structures to conceal beneficial ownership (BO), the creation and management of shell or front companies, asset acquisition through nominees, recruitment of money mules or frontmen, provision of financing or credit, identification of investment opportunities, and facilitation of VA–fiat conversions. These activities are typically organised through cross-border arrangements.

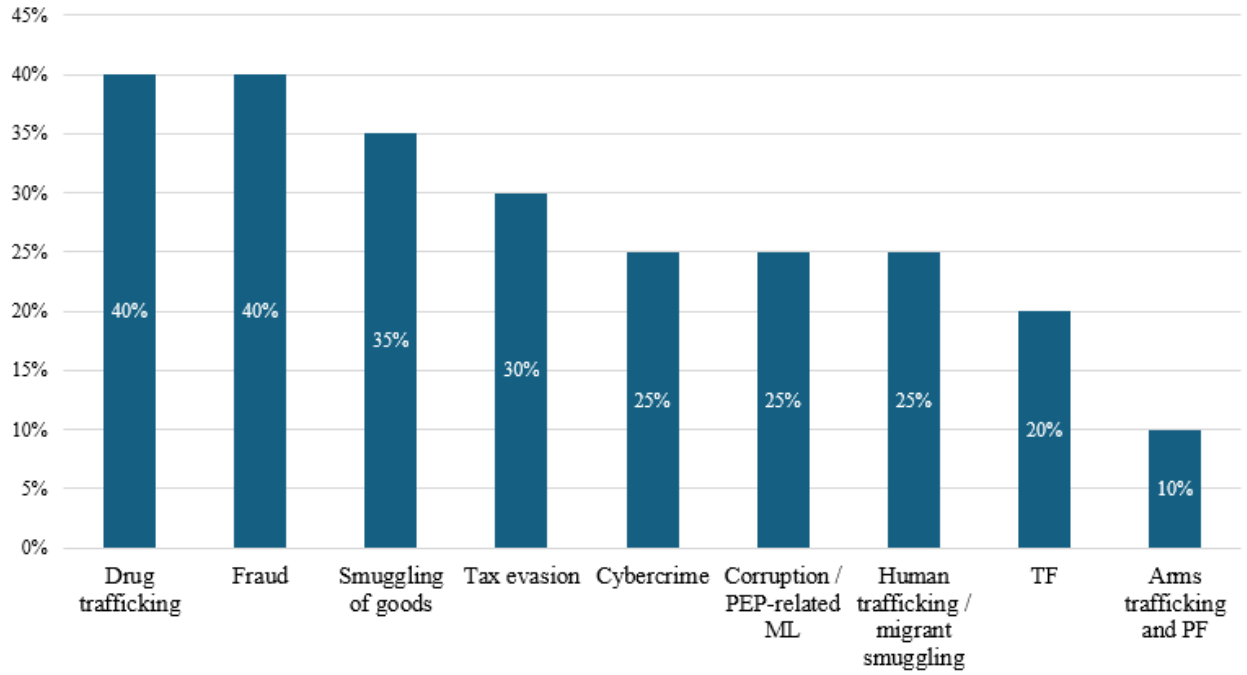
5.4. Predicate offences

62. Across 39 jurisdictions, underground banking and HOSSPs are reported to be used to launder proceeds derived from a broad range of predicate offences.

[10] FATF (2013), *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

Infographic 4. Main predicate offences associated with PML involving underground banking and HOSSPs

Percentage of jurisdictions responding to the survey identifying each offence:



63. The principal offences identified include drug trafficking (see Box 1), fraud, smuggling of goods, tax evasion, cybercrime, corruption, as well as human trafficking and migrant smuggling. These findings are broadly consistent with INTERPOL's 2025 global survey, which identifies—in descending order—tax evasion, drug trafficking, corruption, organised retail crime and counterfeiting, human trafficking and migrant smuggling, TF, cyber-enabled financial fraud, and environmental crime.

Box 1. Use of underground banking systems and HOSSP-based PML schemes in drug trafficking

Netherlands: Operation Klaver exposed one of the largest underground banking networks identified in the Netherlands and Europe. Over an eight-month period, the network processed approximately EUR 500 million in criminal proceeds, largely on behalf of drug-trafficking organisations. The network operated as a cash-based informal value-transfer system. Couriers collected large sums of cash from criminal clients, delivered the funds to warehouses for counting and recording, and then redistributed equivalent amounts to other criminal actors. These collection and delivery mechanisms enabled drug-trafficking groups to pool, move, and reallocate proceeds without using the formal financial sector. The scheme also displayed features of PML. Transactions were tracked through internal records and coded references, while commissions, logistics, cash storage, and courier movements were organised in a manner similar to a financial service provider. The network co-ordinated with international money brokers to balance accounts

across jurisdictions, allowing value to be transferred to source and transit countries and used to finance further drug shipments.

64. Jurisdictions emphasise that proceeds from nearly all types of crime may be laundered through underground banking and HOSSPs. These systems are no longer exclusively associated with traditional cash-intensive crimes such as drug trafficking or smuggling, but increasingly serve as ML infrastructures for a wider spectrum of criminal economies, including fraud, cyber-enabled crime, corruption, tax evasion, TF (see subsection 7.1.4.), undeclared work, illegal gaming and gambling, sanctions evasion, intellectual property crime and counterfeit trade, environmental crime, illegal resource extraction, extortion, kidnapping for ransom, burglary/theft, and transnational organised crime generating proceeds from diverse activities. These predicate offences may be committed domestically or abroad, and the proceeds are frequently co-mingled with funds of lawful origin.

Box 2. Underground banking and HOSSPs used by criminal networks to launder proceeds and facilitate undeclared work

Belgium identified underground banking and HOSSP-based schemes in which criminal groups holding illicit cash, including from drug trafficking and illegal trade, exchange that cash with businesses seeking undeclared funds to pay workers off the books. These arrangements have been observed in sectors such as construction, cleaning, and transport, where cash may be used to evade payroll taxes and social security contributions. The scheme operates as a compensation mechanism. Criminal cash is transferred hand-to-hand or through informal money or value transfer channels to company directors or intermediaries that need cash. In return, equivalent value is sent through bank transfers, often to domestic or foreign accounts controlled by the original criminal group. These transfers are typically supported by false invoices and vague payment references, such as purchases of goods or settlement of invoices. Intermediary companies may be shell entities or businesses with genuine activity, particularly in cash-generating sectors where undeclared economic activity is easier to conceal. The typology allows one criminal actor to dispose of illicit cash while another obtains unrecorded cash for labour or operating costs.

6. Settlement methods

65. This subsection examines how underground banking operators and HOSSPs settle outstanding balances between themselves and provides country examples in the context of their criminal misuse for PML.

66. The 2013 FATF report on *The Role of Hawala and Other Similar Service Providers in ML/TF* identified five core mechanisms: simple reverse (offsetting) transactions; triangular or network-based settlements; settlement through equivalent value; settlement via formal financial channels, and cash-based settlement.

67. A decade later, drawing on responses to the 2025 FATF Global Network survey, this report revisits and refines that typology to reflect current practices and technological developments. The updated framework remains focused on settlement

mechanisms—i.e. how obligations between service providers are discharged and how cash pools are rebalanced—rather than on the form of value transfer. One exception is the introduction of a fifth category, digitally based settlement, reflecting the growing use of VAs in PML schemes, a trend also highlighted in the FATF's recent update on TF risks. The revised typology further underscores the continued, and in some jurisdictions increasing, reliance on formal banking channels for settlement. These five categories are analytical in nature, not mutually exclusive, and may coexist or be combined within a single underground banking or HOSSP-related PML scheme.

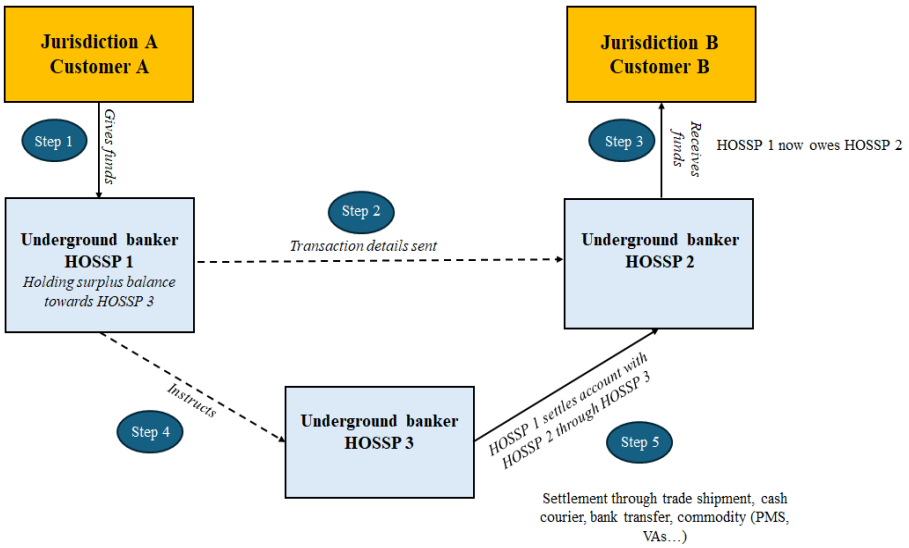
6.1. Simple reverse transactions (bilateral offsetting)

68. In its most basic form, settlement occurs through direct, bilateral offsetting of obligations between two service providers. Funds paid out by HOSSP 1 in one jurisdiction are balanced by funds paid out by HOSSP 2 in another. No physical of financial settlement is required where flows are symmetrical (see Infographic 2). This mechanism is the fundamental of all systems and remains common in all regions.

6.2. Triangular / network-based settlements

69. A core method in contemporary underground banking and HOSSPs involves multilateral compensation across a network of brokers, in which balances between HOSSPs are settled indirectly through third jurisdictions. For example, HOSSP 1 in Jurisdiction A may owe HOSSP 2 in Jurisdiction B. However, the obligation is extinguished through HOSSP 3, which may hold surplus balances, facilitate trade-based settlement, move value through cash or other mechanisms, or offset the liability against separate obligations within the network. Such triangular or multi-node settlement increases opacity and reduces traceability. In large HOSSP networks, multi-node settlement could plausibly also be conducted through a central office that tracks all debits and credits across the network to simplify repayment.

Infographic 5. Triangular settlement



70. A related manifestation involves clearing via third-party transfers i.e. the settlement of balances through unconnected third parties. Rather than HOSSPs

settling directly with one another, debts are cleared by arranging or directing payments of invoices, commercial obligations, repayment of debts or other financial transfers conducted by third parties. Third-party payments do not constitute a standalone settlement modality. Rather, they represent a commonly used technique through which network-based, value-based (including trade-based mechanisms), or formal-channel settlement is carried out.

6.3. Settlement through value (cash couriers, trade-based, in-kind including precious metals and stones)

71. Many underground banking networks and HOSSPs settle obligations through the transfer of equivalent value, rather than by directly transferring funds (see Box 3). Such settlement mechanisms include:

(i) Cash couriers, namely individuals who physically transport cash or bearer negotiable instruments on behalf of others, often across borders, to rebalance positions between service providers;

(ii) Trade-based mechanisms, including over- and under-invoicing, falsified or manipulated shipping documents, invoice manipulation, and phantom shipments. In trade-based settlement schemes, underground bankers or HOSSPs use import–export front companies to manipulate invoices—through over- or under-invoicing and falsified cargo descriptions—to balance inter-operator accounts via fictitious trade transactions. Such companies, typically operating in cash-intensive sectors (e.g. vehicle sales or luxury goods), often exhibit frequent cash deposits. Disguising criminal proceeds as legitimate trade flows is a widely used settlement method in underground banking- and HOSSP-based PML schemes. In cross-border trade-based PML schemes, a distinction exists between third-party payments—where the exporter is paid by an entity other than the invoiced customer, often controlled by the PML network—and TBML itself, which involves discrepancies between the actual value of goods and the declared value used to justify payments. A further distinction arises between payments made via standard bank transfers and those executed through trade-specific instruments, such as documentary credits and international guarantees.

(iii) Commodity-based offsets, involving the use of consumer goods, gold, or other precious metals to transfer or store value and settle outstanding balances between operators. Meanwhile, the commodity-based offset is extended to the field of high-value luxury goods, in which criminal cash is converted into luxury goods for cross-border transfer, and the settlement of outstanding balances is realised through the repurchase and resale of luxury goods, forming a commodity-based settlement model combining value transfer and physical commodity circulation.

(iv) Three-way exchange and mirror-transaction models, in which illicit funds generated in one jurisdiction are exchanged for local funds from individuals seeking to transfer value overseas (e.g. to circumvent capital controls). These local funds are then used to purchase goods that are exported and sold abroad to generate foreign-currency value, thereby completing the full value cycle and enabling cross-border value transfer without any bank-recorded movement of funds.

72. A specific regional variant involves parallel-currency or peso-based mechanisms, in which HOSSPs leverage black-market or parallel foreign-exchange rates to clear cross-border obligations. These arrangements—such as BMPE-type systems—combine trade, foreign exchange (FX) arbitrage, and informal value transfer, and are particularly relevant in jurisdictions with significant parallel exchange markets (see subsection 7.2.3).

Box 3. Country examples of settlements through value

Belgium: Cash courier–based settlements

A Europol-supported investigation identified an underground banking network suspected of laundering cocaine-trafficking proceeds through cash courier-based settlement. The network operated across Belgium, the Netherlands, Spain, Morocco, South America, and Dubai. The scheme relied on physical cash movement between service providers. Drug proceeds were transported from Belgium to a safe house in Amsterdam in vehicles fitted with hidden compartments. A separate criminal service provider then arranged onward cash transport to Spain. The funds were subsequently delivered to illegal currency exchange offices, which settled equivalent value in Morocco for a commission. The laundered proceeds were later invested in luxury real estate projects in Europe and Morocco.

India: Trade-based money laundering through shell companies

In March 2022, Indian authorities identified a transnational PML scheme that used shell companies and trade transactions to transfer value across jurisdictions. The companies were incorporated through nominees, often using stolen or forged Know your customer (KYC) documents, and had limited or no genuine business activity. The scheme combined under-invoicing, circular trade, and outward remittances. Trading entities imported genuine goods at deliberately understated values, leaving an undisclosed balance payable abroad. Domestic shell companies then used forged trade documentation to justify additional outward remittances to related shell companies in another jurisdiction, under the appearance of legitimate import transactions. The network also used circular trade flows. Goods were exported to related entities in a third jurisdiction, where payment was deliberately withheld on the basis of fictitious commercial disputes, before the goods were re-exported to entities controlled by the same network.

6.4. Formal-channel/bank-based settlement

73. Despite the informal nature of underground banking and HOSSP operations, many networks continue to rely on the regulated financial system to settle net balances. Settlement may be disguised as legitimate commercial activity and facilitated through shell companies, money-mule accounts, virtual IBANs (vIBANs), or corporate structures. Wire transfers, batch payments, and layered transactions are common features.

74. Third party money mules are commonly used to fragment large-sum criminal cash into multiple small deposits and transfer them to designated accounts, avoiding the AML monitoring thresholds of FIs.

75. Another frequently reported method is 'cuckoo smurfing', a form of third-party payment whereby illicit cash is deposited into the bank account of an unsuspecting legitimate remitter. The remitter's genuine outbound transfer is then used to settle obligations offshore, while the structured cash deposits are used to balance domestic payouts. In effect, the criminal network settles accounts through the banking system while obscuring the origin of funds and the true purpose of the transfer.

76. Another variant of formal-channel and network-based settlement, may be the use of crowdfunding platforms as a pooling and narrative mechanism to disguise third-party clearing of obligations between underground banking and HOSSP operators (see Box 4). Crowdfunding platforms are digital platforms through which funds are channelled via PSPs, MVTS, bank accounts, cards, or comparable instruments. From a settlement perspective, obligations between underground bankers or HOSSPs are extinguished / executed using formal financial rails, even where the underlying economic purpose of the transactions is fictitious or misrepresented. Typically, an obligation owed by HOSSP 1 to HOSSP 2 is settled when funds raised through a crowdfunding campaign—controlled directly or indirectly by the network—are transferred via PSPs or banking channels, with the settlement obscured by the appearance of legitimate donations, loans, or investment activity.

Box 4. Crowdfunding used as a formal-channel (bank-based) settlement layer

Germany: German authorities identified HOSSP-related schemes in which crowdfunding or donation campaigns were used to create a legitimate-looking payment narrative for underground banking settlements. In one variant, a campaign initiator received donations through a crowdfunding platform and diverted the funds to settle obligations within an underground banking network, rather than using them for the stated charitable or humanitarian purpose. In another variant, third-party funds, including cash deposits from persons linked to cash-intensive businesses, were first aggregated in a bank account and then transferred to a crowdfunding campaign as apparent donations. In both variants, the crowdfunding platform, payment service provider or MVTS created a bank-visible explanation for the movement of funds. Cash-intensive businesses, such as kiosks, hookah bars, mobile phone shops or souvenir shops, provided cover for cash deposits, third-party payments, and mixed funding sources.

6.5. Digitally-based settlement

77. Increasingly, obligations between HOSSPs are settled using digital value-transfer mechanisms, including VAs (particularly stablecoins to reduce price volatility), online PSPs, and digital banking platforms. These tools enable near-instant compensation across jurisdictions, reduce the need for physical cash movement, and can be used in combination with traditional settlement methods to layer or integrate illicit proceeds (see Box 5).

78. Digital-enabled value-transfer mechanisms do not constitute a distinct settlement modality in themselves. Rather, they operate as a cross-cutting enabler that can support, facilitate, or accelerate other settlement mechanisms while offering HOSSPs enhanced speed, global reach, and perceived anonymity.

Box 5. VA-based settlements in underground banking- and HOSSP-based PML

Türkiye identified a shift from traditional cash-based hawala settlement towards technology-enabled models using VAs, particularly stablecoins such as USDT. In these schemes, underground banking operators and HOSSPs use virtual asset service providers (VASPs), over-the-counter brokers, payment institutions, and bank accounts to transfer and settle value across jurisdictions. The model relies on fiat collection, conversion into VAs, wallet-to-wallet transfers, and conversion back into fiat or other stores of value. Mule accounts, including accounts held by young persons or migrants, are used across banks, payment institutions, and VASPs to receive and move funds. Some networks may also use exchange offices, jewellery businesses, precious metals transactions, and front companies to simulate legitimate commercial activity or provide alternative settlement routes.

7. Emerging typologies and trends

79. Nearly 70% of the responding jurisdictions reported observing emerging typologies and trends in the misuse of underground banking and HOSSPs for PML, confirming that this is a rapidly evolving landscape. This subsection seeks to identify and outline these developments. The analysis of questionnaire responses points to two overarching dynamics: first, converging global trends, and second, persisting or newly emerging regional patterns.

7.1. Global convergences

7.1.1. Digitalisation

80. The digital transformation of underground banking and HOSSPs is one of the most significant global developments in their use for PML. While some jurisdictions continue to report reliance on traditional face-to-face mechanisms, nearly 70% of respondents identify the integration of new technologies, with a growing shift towards what is often termed "digital hawala".

81. "Digital hawala" broadly refers to the use of digital technologies to facilitate the co-ordination, execution, settlement, or concealment of informal value transfer. The term is applied inconsistently across jurisdictions and covers a spectrum of practices, ranging from digital communication tools to full integration of VAs and digital payment systems. In practice, several core configurations are observed:

(i) **Digital co-ordination, traditional settlement**: Operators use encrypted messaging applications (e.g. WhatsApp, Telegram, Signal) and digital tools (including shared ledgers or online platforms) to co-ordinate transactions, communicate instructions, recruit clients or couriers, and maintain records. These communications are often ephemeral, encrypted, and fragmented across platforms and jurisdictions. Despite this digital layer, settlement continues through traditional mechanisms (cash or trade).

(ii) **Digital customer interface, traditional inter-operator settlement**: Customers initiate transfers through bank transfers, mobile wallets, fintech applications, or instant payment systems, while settlement between

operators remains based on cash, trade, or other conventional offsetting mechanisms.

(iii) **Use of VAs for settlement**: In more advanced models, operators use VAs—including stablecoins such as USDT, USDC and DAI—to settle balances between themselves, either replacing or complementing traditional methods. These arrangements may involve rapid VA transfers, VA-to-cash conversions, or hybrid combinations with trade-based or cash settlement (see Box 5).

(iv) **Integration with formal digital financial infrastructure**: Underground banking and HOSSP activity may be embedded within regulated systems, including PSPs, fintech platforms, vIBANs, and online banking channels, which are used to move funds digitally while concealing the underlying informal settlement layer.

(v) **Use of advanced technologies, notably AI-based tools**: Some jurisdictions report the use of AI-based tools to facilitate PML, including automated structuring of transactions, dynamic routing across mule accounts and payment platforms, high-speed fiat–VA conversions, selection and management of mule accounts, and the generation of transaction patterns that mimic legitimate activity (see Box 6).

Box 6. Onboarding of automated tooling in underground banking- and HOSSP-based PML schemes

Japan: Japanese authorities identified the use of automated transfer functions in PML schemes. These tools can be configured to move funds from mule, third-party, or compromised accounts once deposits reach a specified amount. In underground banking- and HOSSP-based schemes, this threshold-triggered "sweeping" helps move funds rapidly through multiple accounts, reducing the time proceeds remain in any single account and limiting manual intervention by operators. The automated transfer may also be followed by conversion into VAs and onward transfer to overseas wallets.

(vi) **'Hawala apps' and bundled digital ecosystems**: Increasingly, operators rely on combinations of digital services—including encrypted messaging, cloud storage, social media, VASPs, lending applications, and gaming platforms—to manage customer onboarding, co-ordination, and settlement. These tools may function as integrated ecosystems rather than standalone applications, enabling cross-border operations with limited visibility, reduced physical presence, and high operational flexibility. In some cases, purpose-built applications have been identified.

82. Jurisdictions identify several key effects of digitalisation that are particularly relevant for detection:

(i) **Increased speed**: Faster customer–operator interaction and accelerated cross-border settlement reduce detection windows.

(ii) **Greater opacity**: Use of encrypted, ephemeral, or unregulated digital environments shifts records away from traceable formats, complicating evidential recovery.

(iii) **More complex layering:** Digital tools enable rapid combination of multiple channels (PSPs, VAs, mule accounts, trade), increasing transaction complexity and hindering reconstruction.

(iv) **Expanded reach and resilience**: Networks operate across jurisdictions with reduced reliance on physical presence, increasing scalability and adaptability.

83. The impact of digitalisation on cash use is mixed. While some jurisdictions report reduced reliance on cash for inter-operator settlement, with a shift towards digital and trade-based methods, cash remains critical at entry (collection) and exit (payout) points. Bulk cash movement, including cross-border transport, continues to play a significant role in certain networks (see subsection 6.3.).

84. Digitalisation is also changing the dynamics of underground banking- and HOSSP-based PML networks. Traditional reliance on personal relationships and community ties is diminishing, with co-ordination and validation increasingly supported by digital tools, transaction records, and system-based verification mechanisms. For competent authorities and private sector stakeholders involved in detecting such schemes, this shift may reduce the relevance of identifiable interpersonal links. Access to these networks is increasingly controlled through technological means, including closed applications, invitation-only platforms, and vetted entry procedures, which operate as digital access controls.

7.1.2. Professionalisation

85. The professionalisation of underground banking and HOSSP-based PML does not refer solely to improved service efficiency, as such networks have long demonstrated effectiveness and reliability. Rather, it denotes a more specific evolution into structured, service-oriented ML infrastructures. This evolution is characterised by increasingly formalised organisational arrangements, specialised roles, standardised processes, and the growing involvement of professional intermediaries and enablers. Collectively, these features reinforce the capacity of such networks to operate as sophisticated ML infrastructures supporting more diversified and complex PML schemes.

86. Several jurisdictions report that underground banking systems and HOSSPs are increasingly organised as business-like structures, incorporating formal management practices, specialised functions, and enhanced operational security. Observed developments include hierarchical or cell-based configurations, the use of corporate-style record-keeping (including digitised ledgers), and reliance on dedicated logistical and technical specialists. While hierarchy is not always fixed, it tends to become more structured as operations scale.

87. A category of highly sophisticated, scalable, and commercially operated cross-border PML networks has emerged. These networks are characterised by cost efficiency, strong liquidity access, and technological innovation, often offering lower commission rates and reduced operational risk compared to traditional channels. Their capacity to move large volumes of value rapidly across borders and to provide end-to-end ML services to organised crime groups—drawing on multidisciplinary expertise—further reinforces the professionalisation and commercialisation of underground banking- and HOSSP-based PML.

88. Jurisdictions also report increasing involvement of professional service providers—including lawyers, accountants, auditors, notaries, corporate formation agents, financial consultants, real estate agents, as well as casinos and junket

operators—in facilitating such schemes. These actors range from established professionals operating lawfully but, knowingly or through wilful blindness, providing occasional services to criminal clients, to individuals operating fully within criminal networks.

89. In a number of suspicious transactions linked to underground banking and PML, competent authorities identify structured transfers of funds of unknown origin to legal professionals, often without clear economic purpose or identifiable relationship between the parties.

90. Overall, this professionalisation trend acts as a significant risk multiplier, enhancing the capability, opacity, and resilience of underground value-transfer networks, and enabling their convergence with TBML, real estate, VAs, and corporate structures.

7.1.3. Deepening integration with the formal financial sector

91. Survey responses indicate a growing degree of interaction between underground banking and HOSSP networks and the formal financial system, reflecting a strategic evolution to increase efficiency and reduce detection risk. Rather than operating entirely outside regulated channels, PML actors increasingly combine informal value-transfer mechanisms with licit financial infrastructures, exploiting regulatory asymmetries and supervisory blind spots. Underground banking and HOSSP activity therefore often involves the concealed use of formal financial products and services, including bank and payment accounts. This is consistent with UNODC findings that contemporary hawaladars increasingly rely on bank accounts to facilitate or settle transactions[11].

92. Jurisdictions report that these networks use formal financial accounts, fintech platforms, payment service providers (PSPs), online banking, and digital wallets as entry and exit points for ML cycles. Underground banking functions as the hidden settlement layer, while the formal sector is used for customer interface, placement, and layering, often through front entities, straw accounts, or mule networks. Even where non-bank payment infrastructures are used, they typically depend on banking access (e.g. safeguarding or settlement accounts), meaning banks remain central to payment flows and liquidity management. Hybrid models combining VAs, digital platforms, and cash pooling are widely observed, illustrating convergence with mainstream financial technologies.

93. Authorities highlight the role of legitimate-appearing legal structures—such as trading firms, import/export companies, and professional intermediaries—as façades enabling access to regulated services. Networks often maintain multiple bank accounts, including those held by nominees or shell entities, and use tools such as vIBANs to facilitate rapid cross-border transfers. In some cases, criminal groups have infiltrated or controlled non-bank payment providers to offer services to other networks. Professional money launderers also target weakly supervised institutions and jurisdictions with limited oversight, and may recruit insiders within the financial sector.

[11] UNODC (2023), *The Hawala System: Its Operations and Misuse by Opiate Traffickers and Migrant Smugglers*, UNODC, Vienna, https://www.unodc.org/documents/data-and-analysis/AOTP/Hawala_Digital.pdf

94. This integration strengthens operational resilience by enabling large-value ML with greater speed and apparent legitimacy, while increasing the complexity of detection and tracing. It demonstrates that underground banking and HOSSP networks rely structurally on formal-sector access to place, transfer, convert, and integrate criminal proceeds, including through mule accounts, bank transfers, VA purchases, and asset acquisition. This underscores the need for enhanced supervisory focus on cross-sectoral interfaces, including banks, PSPs, fintech firms, currency exchanges, and company service providers.

95. Jurisdictions also report the selective but well-established use of prepaid cards and vouchers as bridging instruments between cash-based underground banking arrangements and the formal payment system. These tools enable rapid, low-cost cross-border transfers and access to funds, often without direct banking relationships. Frequently linked to mule accounts or misused identities, they facilitate layering, short-term value storage, and reduced reliance on cash couriers. Their compatibility with ATM and international withdrawal networks allows them to function as cash substitutes at placement and early layering stages. In HOSSP-based schemes, they support movement of value between informal settlement layers and regulated channels, including in digitally enabled typologies and cases linked to TF.

96. Mobile payment terminals present a further vulnerability at this interface. Criminals may deploy terminals through complicit or fictitious businesses to process sham transactions, introducing illicit funds into regulated systems under the guise of legitimate revenue. These infrastructures enable rapid onward, including cross-border, transfers and support layering through transfers to shell entities or conversion into assets such as VAs. By creating an apparent commercial trail, they facilitate the integration of illicit proceeds into the legal economy and illustrate how underground banking and HOSSP networks exploit regulated payment infrastructures while concealing underlying informal settlement mechanisms.

Box 7. Misuse of vIBANs, PSPs, payment agents, and prepaid cards to support underground banking- and HOSSP-based PML schemes

Italy: Italian authorities have identified PML typologies in which underground banking and HOSSP-based schemes are integrated with regulated payment infrastructures, including vIBANs, PSPs, payment agents, and prepaid cards. These tools are used to collect, layer and transfer illicit proceeds, often linked to tax offences, scams, and false invoicing, while obscuring the origin and destination of funds.

vIBANs are increasingly used to mask the true destination of funds or give cross-border transfers the appearance of domestic payments. Multiple 'alias accounts' may route incoming payments to a central master account, creating a nesting effect and shielding illicit activity behind regulated intermediation. Italian authorities have identified cases involving Chinese underground banking networks, where illicit proceeds were transferred abroad through non-EU PSPs using European bank accounts to provide vIBANs to Chinese clients.

Investigations have also identified European Union (EU) payment and e-money institution agents operating under passporting arrangements but acting de facto as

autonomous financial intermediaries and PML facilitators, including in schemes linked to Chinese underground banking networks and misuse of public funds.

In this context, prepaid cards are also used to aggregate illicit funds domestically before transferring them abroad through fragmented transactions to PSPs in other EU Member States, complicating detection while creating identifiable patterns of concentration and routing.

7.1.4. Intersection between underground banking, HOSSP, and TF

97. The 2013 FATF report on the role of HOSSPs in ML and TF already concluded that HOSSPs constitute a significant and persistent vulnerability TF. At that time, a broad consensus had emerged among jurisdictions recognising that underground banking and HOSSPs pose a high TF risk.

98. Over the past decade, the use of HOSSPs by UN-designated terrorist groups has been widely reported by the United Nations 1267 Monitoring Team[12] and, in 2025, the FATF *Comprehensive Update on Terrorist Financing Risks*[13] confirmed that HOSSPs remain a core TF method, particularly in high-risk contexts. The report found that HOSSPs continue to be widely used for TF, notably in conflict and post-conflict zones, remote or underserved areas with limited access to formal financial services, and jurisdictions characterised by large informal and cash-based economies. HOSSPs are especially vulnerable where they operate outside licensing and registration regimes, without customer due diligence (CDD), with limited or no record-keeping, through cash-based settlement and compensation mechanisms, and across porous borders with minimal oversight. Both large networked terrorist organisations and local affiliates continue to rely on underground banking and HOSSP-based mechanisms to receive donations from abroad, move funds between regional hubs, transfer value into and out of conflict areas, and support decentralised cells and operatives. The 2025 report also highlighted an evolution in TF typologies, with HOSSPs increasingly integrated with other TF techniques, including cash smuggling, abuse of non-profit organisations (NPOs), proceeds from criminal activities (such as smuggling, trafficking, and extortion), trade-based terrorist financing (TBTF), and emerging digital adaptations of underground banking and HOSSPs, including the use of encrypted communications and pseudo-anonymous technologies. As a result, underground banking and HOSSPs are rarely used in isolation, but instead function as connective infrastructure within broader TF ecosystems.

99. Responses to the survey confirm these trends.

100. Several jurisdictions report concrete TF cases involving underground banking or HOSSPs, demonstrating that TF through HOSSPs is a tangible risk. Several

[12] See UN Security Council (2022), *Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities*, S/2022/547, 15 July 2022, https://docs.un.org/en/S/2022/547; and UN Security Council (2023), *Thirty-second report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities*, S/2023/549, 25 July 2023, https://docs.un.org/en/S/2023/549.

[13] FATF (2025), *Comprehensive Update on Terrorist Financing Risks*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf

jurisdictions have also identified underground banking and HOSSPs as high risk for both ML and TF in their NRAs.

101. The intersection between TF and HOSSPs often involves the covert movement of funds to support extremist groups in conflict regions or to facilitate related criminal activities. TF through underground banking and HOSSPs is further observed in the Middle East, Asia, and West Africa and is frequently co-mingled with legitimate diaspora remittances, which further complicates detection and disruption particularly for unregulated HOSSPs that do not generally have compliance programs.

102. Finally, digitalisation—notably the hybridisation of traditional underground banking and HOSSP models with the use of VAs and digital tools—appears to act as a catalyst for the use of underground banking and HOSSPs for TF, rather than replacing these mechanisms altogether.

Box 8. Use of HOSSP networks for TF

Türkiye: Türkiye identified a 'digital hawala' network used to finance members of the terrorist organisation Islamic State in Iraq and the Levant (ISIL). The scheme relied on hawala-style transfers supported by digital receipts, front businesses, and high-volume transactions inconsistent with the individuals' financial profiles. In 2023, following intelligence on a so-called general administrative officer of ISIL and his affiliates in Türkiye, LEAs searched his premises and seized approximately USD 57 250 in cash, held in USD, euros, and Turkish liras. Special investigative techniques identified six additional persons sharing common base signals with several individuals with terrorist offence records. Further searches led to the seizure of approximately USD 554 000 in cash, also held in USD, euros, and Turkish liras, as well as notebooks containing hawala records and digital materials. Examination of the seized materials revealed numerous digital hawala transfer receipts from various regions and involving different recipients, including some linked to one ISIL's so-called prison camp. A jeweller and two mobile phone shops were identified as fronts for hawala transactions. MASAK analysis further identified suspicious high-volume money transfers among these individuals, many using 'infak' (charity) as the stated transfer reason.

7.2. Regional patterns and emerging hubs

103. The above-described trends are observed across all FATF regions. At the same time, regional patterns persist/emerge:

7.2.1. Integration of underground banking and HOSSPs with mobile money systems (Africa & Asia)

104. A prominent regional pattern identified through the FATF survey analysis and confirmed by INTERPOL is the integration of underground banking and HOSSPs with mobile-money ecosystems, particularly in Africa and Asia, where mobile wallets and telecom-based financial services are widely used as customer-facing payment channels, enabling users to deposit or withdraw funds through telecom-linked e-wallets or fintech payment platforms.

105. Mobile wallet–based systems increasingly underpin cross-border value transfers within underground banking networks and HOSSPs, giving rise to hybrid models that combine traditional hawala structures with digital retail payment infrastructures (see Box 9). In most cases, mobile money is used by customers to cash in and cash out funds to and from underground banking operators and HOSSPs, with end users experiencing near-instant transfers through mobile wallets. Underlying settlement, however, often occurs off-platform, including through physical cash or trade goods. More occasionally, mobile money is also used by underground banking operators and HOSSPs, such as currency traders, for settlement between cash pools.

106. Several factors facilitate the integration of underground banking and HOSSPs with mobile money systems in Africa and Asia, including:

(i) Regulatory arbitrage in jurisdictions with strict capital controls, limited access to banking services, or burdensome documentation requirements;

(ii) Financial exclusion combined with agent overlap, whereby hawaladars and mobile money agents operate within the same markets and communities; and

(iii) Reliance on affordable and rapid remittance services by diaspora communities and informal cross-border trade corridors across the Sahel, East Africa, the Horn of Africa, and parts of Asia.

107. This convergence between underground banking, HOSSPs, and mobile money has created new challenges associated with disrupting PML.

108. In Asia, jurisdictions report that the convenience, speed, and comparatively weaker due-diligence controls of certain mobile-money environments have increased their attractiveness to professional money launderers. Mobile money facilitates rapid distribution to mule networks and decentralised liquidity points, enabling layering and cash-out operations, frequently in combination with VAs and PSP–enabled payment mechanisms.

109. In Africa, mobile money is deeply embedded in informal financial practices due to high levels of financial exclusion, limited access to banking services, widespread reliance on telecom-based payments, and the fact that, in many cases, it has historically been the main means of formal financial intermediation. While underground banking and HOSSP networks remain predominantly cash-heavy and are often linked to trade, gold, and real estate, mobile-money wallets increasingly serve as entry and exit channels for informal transfers. In several jurisdictions, historically cash-based underground banking and HOSSPs have evolved into hybrid arrangements incorporating mobile wallets for customer-facing transactions, digital ledgers and messaging applications for co-ordination, and extensive agent networks as cash-in and cash-out points. Rather than displacing informal systems, mobile money is increasingly embedded within them to facilitate the placement, layering, and distribution of illicit proceeds.

110. Sub-regional trends regarding the integration of underground banking and HOSSPs with mobile money for PML in Africa include:

(i) East Africa: Underground banking and HOSSPs remain central to cross-border corridors, notably those linked to Somali diaspora remittances. Transactions are settled through mobile money rails (e.g. Kenya's M-Pesa), cash agents, or informal exchangers.

(ii) West Africa: High levels of intra-regional migration and commercial activity have generated dense remittance and trade corridors. Illicit (or unlicensed) FX service providers and underground banking actors in major cities—such as Lagos, Accra, Cotonou, and Abidjan—act as nexus points linking cash-based HOSSP transactions with mobile money transfers and, in some cases, bank accounts.

(iii) North Africa: Conflict dynamics and currency controls serve as catalysts for the growth of informal money or value-transfer services. In these markets, underground banking and HOSSPs are used to bypass restrictions, while mobile money—though less widespread—serves as an emerging settlement layer.

(iv) Southern Africa: Integration between underground banking, HOSSPs, and mobile money systems is less pronounced but growing along migrant remittance routes—particularly between Zimbabwe and South Africa and between Mozambique and South Africa.

111. Underground banking systems and HOSSPs historically established in the Middle East and South Asia are also increasingly connected to African routes through migrant remittances, particularly to East Africa, the Horn of Africa, and parts of West Africa. These networks often involve merchants or diaspora intermediaries holding accounts within both formal banking institutions and mobile money platforms, while continuing to rely on traditional settlement methods. As a result, multi-jurisdictional networks emerge in which part of the value transfer is transparent (e.g. bank-to-mobile wallet transactions), while another segment remains concealed, such as settlement between underground bankers and HOSSPs.

112. Although the growing integration between underground banking, HOSSPs, and mobile money is most strongly developed and structurally embedded in Asia, the Middle East, and Africa, responses to the survey also indicate emerging examples in Europe—where mobile money is reportedly not used as a core settlement instrument.

Box 9. Hawala network using social media and mobile money transfers

Oman: The Central Bank of Oman (CBO) received intelligence through its whistle-blower channel on individuals suspected of operating an unlicensed cross-border remittance business to Pakistan. The reporting entity had detected the activity after observing a sudden reduction in customer remittances through specific corridors. It conducted further enquiries, including customer engagement, joining the relevant WhatsApp group, and collecting supporting evidence before reporting the case.

CBO follow-up enquiries, including social media scanning and off-site analysis, identified a WhatsApp group named "XX Money Exchange", operated by foreign nationals to advertise foreign exchange and remittance services to expatriate communities in Oman. The hawaladars offered rates below the formal market rate, with minimal or no fees, and encouraged customers to share the group with others seeking to remit funds. Customers transferred funds to the suspected hawaladars either in cash or through mobile-linked transfers. The hawaladars then sent screenshots evidencing payment through an e-wallet to a corresponding e-wallet maintained with a payment service provider in Jurisdiction A. The scheme exploited lower-cost remittance channels in destination countries, including fee-free transfers to Pakistan through channels such as RAAST, as well as exchange-rate differentials offered by some digital wallet or payment providers. This allowed the hawaladars to generate margins while offering cheaper remittance services. Omani authorities identified six suspected individuals believed to form a connected network of hawaladars and transaction flows of approximately USD 72 293 over one year.

7.2.2. Hybrid settlements combining VAs and gold (Middle East)

113. Survey analysis reveals a distinct regional pattern in the Middle East involving the integration of VAs and gold within settlement mechanisms used by underground banking and HOSSP networks. Jurisdictions in the region report hybrid models in which value transferred through underground banking and HOSSPs is ultimately balanced through VA transactions backed by gold or other high-value commodities, rather than through traditional cash-based reconciliation (see Box 3). These mechanisms are described as increasingly replacing or complementing historical

settlement approaches such as physical cash movements and trade-based adjustments.

114. In these hybrid structures, gold functions both as a reserve asset underpinning VA settlement balances and as a physical medium used to reconcile outstanding obligations between HOSSPs, particularly in environments characterised by currency instability, capital restrictions, or regulatory constraints. Gold and precious stones may be used as integral settlement instruments to anchor VA transfers within underground banking and HOSSP networks. In the Middle East, precious metals remain important value stores in cash-intensive and trade-based settlement ecosystems.

115. VA-based settlement mechanisms are also becoming increasingly common, reflecting a gradual transition away from exclusive reliance on cash couriering and traditional informal transfer channels. These arrangements are often embedded within multi-layered settlement structures that combine VA transfers, gold-backed value stabilisation, and trade or high-value-goods offsets. Together, these features reduce exposure and risk for criminal HOSSPs and limit opportunities for law enforcement intervention as value is transferred and balances are settled.

116. While hybrid settlement combining VAs and gold appears most established and structurally embedded in the Middle East, related developments are emerging in other regions. Jurisdictions in Europe, Asia, and parts of Africa report the rise of hybrid models combining VA transfers with trade-based settlement, although these do not presently display the systematic gold-backing observed in the Middle East. This suggests regional differentiation, where similar technological and operational tools are deployed, but with gold-anchored settlement remaining strongly concentrated in Middle Eastern informal financial ecosystems.

Box 10. Hybrid settlement models combining VAs and precious metals and stones

Türkiye identified a 'digital hawala' typology in which underground banking and HOSSP networks used both VAs and precious metals or stones to transfer and settle value. The network used multiple channels, including banks, VASPs, over-the-counter VA transactions, foreign-exchange operators, and dealers in precious metals and stones. VAs supported rapid cross-border value transfer and balancing, while gold and other high-value commodities were used to reconcile obligations between operators. The scheme also involved legal entities and related persons, suggesting the use of commercial relationships or corporate accounts to support settlement activity and disguise the informal value-transfer function.

7.2.3. Black market peso exchange and related trade-based underground banking schemes (Latin America)

117. The Black Market Peso Exchange (BMPE) remains a well-established regional ML mechanism in Latin America. While some authorities report that other high-capacity PML networks have become increasingly prominent providers of ML services for major predicate offences (see subsection 7.2.4.), BMPE continues to be identified as a relevant trade- and currency-based ML mechanism in the region.

118. As described in the 2013 FATF report on the role of HOSSPs in ML and TF[14], BMPE mirrors underground banking and HOSSP systems by transferring value across borders without the physical movement of funds, relying instead on commercial trade flows to settle obligations.

119. Trade-based settlement mechanisms involving commodity offsetting—central to BMPE—continue to be observed across multiple jurisdictions in the Americas and Europe. Responses to the survey indicate ML channels linked to cocaine proceeds and trade-based repatriation schemes spanning Latin America, Europe, and the Middle East. Although BMPE was not always explicitly identified, the analysis highlights cross-border movement of cocaine-related proceeds through exchange networks and trade-settlement channels, commodity offsetting across the Americas, Europe, and MENA, and the extensive use of shell and front companies—features consistent with BMPE-style ML structures.

120. BMPE remains a persistent, large-scale regional trend widely recognised by law enforcement and international partners. Its continued use is driven by structural economic factors, including cash-intensive illicit markets, restrictions and costs within formal foreign-exchange systems, longstanding commercial corridors linking Latin America, North America, and East Asia, and the availability of trade flows that facilitate co-mingling.

121. Evidence from the survey further suggests that BMPE-style hybrid settlements are increasingly embedded within multiparty cross-border ML networks and combined with other contemporary channels, including VA-based settlement and trade offsetting.

122. Despite these developments, BMPE remains primarily a Latin American phenomenon. Comparable trade-offset models are reported in West Africa and parts of Asia through commodity-based settlement, although these do not exhibit the peso-exchange pricing structure characteristic of BMPE.

Box 11. Exploitation of government-controlled exchange rates through underground banking mechanisms

Netherlands: Operation Cymbal identified a PML scheme that exploited Venezuela's controlled exchange-rate system through mechanisms comparable to underground banking. Under the scheme, customers travelled to Curaçao and used credit cards to conduct transactions that generated cash in US dollars in exchange for a commission. False invoices for goods such as pharmaceuticals and clothing were used to simulate legitimate purchases, although no goods were delivered. The customers then repatriated the cash to Venezuela and sold it on the parallel market, profiting from the exchange-rate differential. Although formal payment instruments were used, the economic substance was informal value transfer. The credit-card transactions operated as settlement instructions, while operators

[14] FATF (2013), *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, FATF, Paris, France, p. 37, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

provided cash abroad and used false trade documentation to conceal the absence of genuine commercial activity.

7.2.4. High-capacity transnational PML networks rooted in geographic and demographic ties

123. Survey responses indicate that underground banking and HOSSP-based PML is often conducted through networks historically rooted in shared geographic, cultural or community ties. These networks operate transnationally and are reported across all FATF regions. While many originated in community-based remittance practices, in the PML context they have evolved into sophisticated, scalable, and commercially organised service providers capable of moving large volumes of value rapidly across borders.

124. Jurisdictions also identify a distinct and growing pattern involving PML networks with operational links to East Asia, including money launderers in these jurisdictions, facilitators based in the region and/or abroad, related settlement corridors, liquidity channels linked to capital-control circumvention, and trade or value-transfer links. These networks are referred to by some law-enforcement agencies in jurisdictions including the United Kingdom and in the United States as "Chinese-speaking money laundering networks"[15] or "Chinese money laundering organisations/networks"[16]. These transnational organised crime networks may involve participants from multiple jurisdictions.

125. One-third of jurisdictions responding to the survey referenced underground banking and HOSSP structures involving such networks, which are increasingly recognised as significant actors within high-capacity underground banking and HOSSP ecosystems, as well as scalable, commercially organised PML service providers. In their contemporary criminal use, these structures are not community remittance channels, but industrialised ML networks serving multiple criminal and non-criminal clients. They may act as hubs within broader multi-ethnic ML ecosystems (see Box 12), aggregating criminal cash from diverse organised crime groups. Their reported advantages include cost efficiency, access to liquidity, operational flexibility and technological innovation. In some regions, they have displaced traditional BMPE brokers by offering lower commission rates and reduced operational risk.

126. In Europe, Europol's EFIPPP identifies these networks as among the fastest-growing ML infrastructures. Authorities report industrial-scale cash consolidation hubs collecting criminal proceeds, notably from drug trafficking, counterfeit goods markets, and cyber-fraud. These proceeds are redistributed through underground settlement chains and integrated into legitimate-appearing wholesale trading,

[15] See: National Crime Agency (2025), *National Strategic Assessment 2025 of Serious and Organised Crime*, London, 2025, https://www.nationalcrimeagency.gov.uk/images/campaign/NSA/2024/NSA%202025%20Website%20-%20PDF%20Version%20v1.0.pdf.

[16] See: U.S. Department of the Treasury (2024), *2024 National Money Laundering Risk Assessment*, Washington, D.C., February 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf; FinCEN (2025), Financial Trend Analysis, Financial Crimes Enforcement Network, August 2025, https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf; FinCEN (2025), *Advisory*, FIN-2025-A003, Financial Crimes Enforcement Network, 28 August 2025, https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.

textiles, logistics and retail distribution sectors. The United Kingdom and the United States have also highlighted comparable patterns[17]. Related typologies are observed in Asia-Pacific, as well as in Africa and Latin America. In Southeast Asia, for example, such networks may serve drug traffickers, cyber-fraud networks, tax evaders, traders, and individuals seeking to circumvent capital controls. Jurisdictions have developed and implemented strategies to mitigate them.

127. Survey analysis identifies several recurring typologies, often combined in hybrid models:

(i) Industrial-scale collection of criminal cash followed by redistribution through informal settlement chains;

(ii) Use of import/export fronts and wholesale trading structures to balance accounts through over- or under-invoicing, falsified cargo descriptions and commercial offsets;

(iii) Three-way exchange in which cartel-generated US dollars are sold to individuals seeking to circumvent capital controls. RMB is provided in return and used to purchase goods exported and sold abroad, generating euros, pesos or other currencies;

(iv) Daigou-style luxury-goods repurchase networks, whereby criminal cash is converted into high-value goods purchased in Europe and resold in Asia;

(v) Casino and junket-related value transfer, used to insert cash into the formal financial system or move value through gambling-related arrangements;

(vi) Money mule networks, including students or temporary residents abroad, used to fragment deposits and reduce suspicion;

(vii) VA-enabled settlement, often combined with trade settlement, cash pooling or cash payout arrangements; and

(viii) Misuse of regulated payment infrastructure, including PSPs and vIBANs (see Box 7).

128. These typologies demonstrate core features of underground banking and HOSSP-based PML: informal cross-border settlement; settlement outside, alongside or through parts of the regulated financial sector; immediate liquidity through distributed cash pools across jurisdictions; fragmented, informal and encrypted records, often co-ordinated through WhatsApp, WeChat or Telegram; and multi-client ML services.

Box 12. Division of roles across transnational underground banking networks using cash and VA settlement

Spain: In 2025, Operation Karasu identified a structured underground banking network with a clear division of roles between two branches. One branch, of Chinese origin, provided and distributed cash in Spain in exchange for VA payments. Its members acted as couriers, collecting and transporting concealed cash and delivering it to designated recipients following instructions. The second

[17] See footnotes 15 and 16.

branch, of Arab origin, received funds in different jurisdictions and settled the equivalent value by arranging cash payouts in Spain. VA transfers were used to compensate the cash-providing branch, allowing the network to balance obligations without direct bank transfers. Investigators documented 32 transactions totalling more than EUR 5.5 million over three months. One VA address used by the network processed more than USD 21 million over two years, indicating repeated use of the same settlement infrastructure. The case illustrates how HOSSP-based PML can allocate specialised functions across transnational networks, combining cash couriers, concealed cash transport, VA wallets, cross-border offsetting, and cash-for-VA settlement to move value outside the regulated financial system.

7.2.5. Emerging global hubs

129. Analysis of the survey responses highlights the emergence of a regional hub structure within underground banking and HOSSP-related PML activity. This structure is characterised by jurisdictions or geographic clusters that play a recurrent and functional role in the cross-border settlement, clearing or absorption of illicit value within transnational informal value-transfer networks. These hubs operate as nodes within a wider network architecture, concentrating specific stages of the ML process—such as cash aggregation, offsetting, trade-based settlement, VA rebalancing, or formal-channel clearing—rather than serving merely as transit points. This hub-based configuration reflects a broader global division between placement and settlement zones: Europe and West Africa function primarily as cash-generation regions, where illicit proceeds are collected before being channelled abroad, while Asia and the Middle East operate as key financial and operational hubs where cross-border settlement activity is concentrated.

130. The analysis of the case studies provided by the respondent jurisdictions draws an explicit distinction between outgoing hubs, where illicit proceeds are generated and exported for settlement and incoming hubs, where value is received and absorbed through informal settlement systems.

Section 2 – Challenges in combating the use of underground banking and HOSSPs in professional money laundering

8. Fragmented definitions

131. Responses to the survey demonstrated significant fragmentation in the terminology and definitions used to describe underground banking and HOSSPs. This may be the key crux of the issue, creating operational, analytical, and policy challenges. While 'hawala' is the dominant global descriptor, the survey highlights substantial regional and linguistic variation that limits comparability and consistency in risk assessment. Jurisdictions report a wide range of culturally rooted terms, while others rely on technical or regulatory classifications (e.g. 'informal value-transfer system', 'unlicensed money service operator' or 'unauthorised payment service'). Some jurisdictions apply distinct conceptual definitions that differ from widely used informal descriptors, whereas others report no recognised terminology at all. Notably, the survey also reveals intra-jurisdictional inconsistency, with different competent authorities within the same jurisdiction employing different terms or definitions to refer to underground banking systems and HOSSPs. Such divergence may signal gaps in inter-agency co-ordination, inadequate typology dissemination, or disparate operational awareness across agencies. These variations, both between and within jurisdictions, impede shared understanding and complicate co-operation, typology development and intelligence alignment, undermining efforts to develop a coherent and proportionate AML/CFT response.

9. Knowledge gaps, including weaknesses in national risk assessments

132. Survey responses highlight significant knowledge and data gaps that constrain jurisdictions' ability to assess, detect, and disrupt PML involving underground banking and HOSSPs. Many jurisdictions report limited visibility of how these systems operate, including their scale, client profiles, and typologies. This lack of visibility is further compounded by common detection limitations, such as the covert nature of activity, limited data availability, and uneven detection and reporting capacities. INTERPOL similarly identifies the difficulty of detecting and tracing financial flows as the primary barrier to disrupting the criminal use of underground banking and HOSSPs.

133. Across the Global Network, most jurisdictions report no reliable quantitative data on the size or scale of underground banking and HOSSPs, including the number of operators, transaction volumes, market share relative to formal MVTS, or the proportion of PML routed through these systems. Many responses explicitly stated "no data", "no statistics available" or "not sure", even where such systems are recognised as high risk or significant in financial flows. Very few jurisdictions could provide demographic or sectoral profiles of providers or users; where available, information was largely anecdotal and case-driven. Several respondents also noted limited visibility of regional and cross-border flows, relying on isolated investigations rather than consolidated intelligence, reflecting constraints linked to limited data and uneven detection capacities.

134. Multiple jurisdictions reported a lack of detailed typologies on how PML is conducted through underground banking and HOSSPs, particularly regarding

complex settlement mechanisms (e.g. trade-based, third-party clearing), digital adaptations, and hybrid models involving real estate, high-value goods or professional intermediaries. Data are often fragmented across agencies, and cases are not systematically coded to enable extraction of relevant patterns. Several jurisdictions acknowledged incomplete understanding of PML networks, digitalisation and VA-based settlement, and regional typologies such as BMPE variants, VA–gold hybrids, and hawala apps, partly due to the covert nature of activity and fragmented detection frameworks.

135. Knowledge gaps also contribute to training and expertise deficits. Fewer than half of jurisdictions report structured capacity-building on underground banking and HOSSPs, and only about one-third include specific coverage of PML involving these systems. Training is often general or theoretical, with limited focus on local risk understanding. Expertise is frequently concentrated within a small number of specialists (often in FIUs or select law enforcement units), with limited dissemination across supervisory, investigative, and prosecutorial authorities.

136. These limitations are reflected in incomplete or uneven incorporation of underground banking and HOSSP risks in NRAs. While a majority of jurisdictions include these risks, a significant minority do not or are unsure. Where covered, assessments are often high-level and descriptive, with limited quantitative analysis of scale, typology-specific risks, or the role of these systems in PML. Several jurisdictions acknowledge that NRA coverage is outdated and does not reflect developments such as digitalisation, VA-based settlement or mobile-money integration.

137. In some cases, competent authorities within the same jurisdiction hold divergent views on the risk level or regulatory status of underground banking and HOSSPs, indicating limited internal co-ordination. Several responses note that risk classifications are driven by lack of information rather than evidence, with systems sometimes assessed as lower risk due to the absence of identified cases or systematic data collection.

138. Overall, knowledge gaps and weaknesses in NRAs remain a foundational challenge to addressing the misuse of underground banking and HOSSPs for PML, limiting jurisdictions' ability to develop proportionate policies, allocate resources effectively and design targeted supervisory and enforcement responses. These challenges are further exacerbated by systemic detection limitations, including the covert nature of activity, limited data availability, and uneven detection and reporting capacities across jurisdictions.

10. Regulatory asymmetries and challenges

139. Survey responses indicate that regulatory asymmetries represent a major obstacle to effectively addressing the misuse of underground banking and HOSSPs for PML. Jurisdictions report substantial differences in the legal and supervisory treatment of these systems, with underground banking and HOSSPs variously described as: subject to AML/CFT laws but operating without the required licence or registration; fully integrated into AML/CFT frameworks and subject to registration and supervision; or neither explicitly regulated under AML/CFT laws nor prohibited, and therefore operating lawfully without registration.

140. Several responses highlight inconsistent or unclear legal status—both across jurisdictions and within individual jurisdictions—which complicates regulation and

enforcement, creates grey areas, and facilitates the continued operation of informal financial networks. In many jurisdictions, licensing frameworks either do not exist, are ambiguous, or apply only to formal MVTS providers, leaving underground operators outside supervisory reach despite providing equivalent services. Others describe structural supervision gaps arising from limited coverage, insufficient enforcement capacity, or challenges detecting and controlling dispersed and informal operators.

141. The analysis also identifies intra-jurisdictional inconsistency, with different competent authorities applying divergent interpretations of what constitutes a regulated or illegal activity. This fragmentation results in uneven prioritisation and weak co-ordination across supervisory, investigative and prosecutorial functions.

142. Challenges arise not only from deficiencies within individual jurisdictions' regulatory frameworks, but also from gaps and co-ordination issues between regulatory frameworks. Several jurisdictions note that regulatory asymmetries create arbitrage opportunities that are actively exploited by PML networks, which route transactions through jurisdictions with permissive or unclear regimes and minimal monitoring. Differences in requirements for KYC, licensing, record-keeping and reporting enable operators to shift activity rapidly across borders. Respondents also highlight challenges arising from access to the formal financial system: in certain jurisdictions, operators face account closures, difficulties establishing or maintaining banking relationships, and reduced access to correspondent banking services. These conditions have contributed to the growth of unlicensed alternatives. Some respondents explicitly link these dynamics to broader de-risking pressures, which divert legitimate remittance users and some formal MVTS providers into informal channels, thereby increasing opacity and reducing visibility for supervisors and FIUs.

143. Overall, survey findings indicate that uneven legal frameworks, inconsistent supervision and de-risking pressures reinforce the attractiveness of underground banking and HOSSPs for PML networks. These regulatory asymmetries undermine international co-operation, enable jurisdiction-shopping by professional money launderers, and limit jurisdictions' ability to implement proportionate, consistent and effective AML/CFT responses.

11. Operational challenges in detection, investigation, and prosecution

144. Survey responses indicate that jurisdictions face substantial operational challenges in detecting, investigating, and prosecuting PML involving underground banking and HOSSPs. These gaps significantly hinder the ability of competent authorities to identify networks, collect admissible evidence and pursue successful prosecutions, particularly in complex cross-border cases.

145. PML networks most often take the form of a multitude of small teams operating either in co-operation or in competition, depending on client needs. This fragmentation provides them with significant operational flexibility and a high degree of resilience. This characteristic is particularly difficult for LEAs to address, as they must define the scope of investigations with great precision. There is a risk either of dismantling only one team among many—which will be rapidly replaced—or, conversely, of attempting to trace the network's ramifications and thereby over-extending and stalling the investigative and judicial process.

146. Regarding detection, many jurisdictions highlight structural barriers that inhibit proactive detection of PML involving underground banking and HOSSPs. Respondents emphasise the absence of standardised red flags and typologies, especially for emerging digital settlement mechanisms and hybrid cross-border ML models. FIUs report difficulties accessing consistent and standardised intelligence due to fragmented data and insufficient typology sharing. FIUs and LEAs also point to limited capacity to monitor digital components—including fintech channels and VAs—which are increasingly integrated into settlement processes. Jurisdictions indicate a pressing need for behavioural indicators specific to underground banking and HOSSPs to support proactive detection.

147. Several jurisdictions also identify significant operational gaps in conducting complex, multi-jurisdictional investigations involving underground banking and HOSSPs. Responses highlight the limitations of traditional investigative approaches—such as "follow the money," where money does not necessarily move, and infiltration, which is hindered by the community- and diaspora-based nature of many underground banking and HOSSP networks. Existing investigative approaches are often insufficiently technical or lack guidance tailored to these systems, particularly where settlement relies on trade-based mechanisms, account offsetting, commodity-based value transfer or VA components. Jurisdictions request detailed best-practice manuals for investigation, evidence collection and prosecution strategies to strengthen case development and cross-agency co-ordination. Concerns are also raised regarding limited forensic visibility in informal MVTS, which frequently leave no audit trail and rely on culturally embedded relationships, encrypted communications, and cash-intensive processes. These challenges in investigating underground banking/HOSSP activities further complicate investigations into PML activities, where investigators must also establish and distinguish intent and knowledge required for ML offences.

148. Responses to the survey also highlight a range of persistent operational challenges affecting international co-operation, including cross-border complexity, slow mutual legal assistance (MLA) processes, divergent legal frameworks, confidentiality barriers, limited feedback, language and data-format incompatibility, and technology gaps, including in VA tracing. Some jurisdictions report that joint investigations may be constrained by data-sharing restrictions and requirements for mutual consent before information can be acted upon, even where authorities are already co-operating, slowing cross-border action. Differences in legal systems, inconsistent data formats, and confidentiality requirements are key barriers to effective co-operation and can delay the processing of MLA requests, reducing the ability of authorities to respond swiftly to fast-moving investigations involving underground banking and HOSSP-related PML.

149. Jurisdictions also report difficulties in securing effective international co-operation on this topic, noting challenges in engaging certain counterparts despite the transnational nature of these networks.

150. Prosecution challenges are closely linked to gaps in legal frameworks and investigative capability. Respondents report difficulty establishing evidentiary chains for systems operating largely outside formal financial infrastructure and lacking transactional records or legally recognised documentation. Prosecutors highlight challenges explaining informal settlement mechanisms to courts and proving criminal intent where operators claim legitimate remittance or community-based transfer functions—as opposed to being ML activities. Several jurisdictions stress the need for

enhanced international co-operation tools—including MLA templates and joint-investigation models—to support cross-border evidence gathering and judicial co-operation. The survey reflects strong consensus that successful prosecutions require strengthened international interoperability, operational guidance, and deeper integration between FIUs, law enforcement, and prosecutorial authorities.

Section 3 – Good practices in combating the use of underground banking and HOSSPs for professional money laundering

151. This section outlines mitigation approaches and examples of effective practices identified during this study to address the challenges described above and strengthen responses to the use of underground banking and HOSSPs for PML. It highlights a range of areas in which jurisdictions have implemented measures that have proven effective in practice, with a particular focus on enhancing the capabilities and awareness of FIUs, LEAs, prosecutors, and supervisors to detect, disrupt, and dismantle underground banking- and HOSSP-based PML networks (see subsections 15 to 21). These practices are presented as illustrative examples rather than prescriptive requirements, reflecting diverse national contexts and risk profiles. Taken together, they demonstrate that the most effective responses combine legal clarity, institutional co-ordination, capacity-building, preventive measures and proactive enforcement.

12. Establishing a clear and appropriate legal and regulatory environment, and deterring unauthorised activity

152. It is essential that jurisdictions establish a clear and appropriate legal and regulatory environment for underground banking and HOSSPs. One approach is to integrate such services into the formal regulatory regime and subject them to full AML/CFT obligations.

Box 13. Formalising informal MVTS: using licensing/registration to make "invisible" remitters supervisable and less attractive for PML

Sweden treats HOSSPs as money transfer or payment services. Operators providing such services must obtain authorisation from the Swedish Financial Supervisory Authority and are subject to AML/CFT supervision. The supervisor may impose corrective measures, administrative fines, or revoke authorisation where compliance standards are not met.

153. A key corollary is the clear articulation of the illegality of underground banking and HOSSP activities that constitute unauthorised financial services, as well as the applicable regulatory framework and obligations. Given the diversity of terminology and legal approaches across jurisdictions, authorities should clearly define within their banking and/or AML/CFT frameworks which activities are authorised and which are illegal. Such clarity supports consistency and a more level regulatory and enforcement environment.

Box 14. Criminalisation of underground banking and HOSSPs

Bangladesh treats *hundi*, the local term for underground banking and HOSSP-style value transfer, as illegal financial activity rather than as informal or tolerated remittance. The legal framework allows authorities to address *hundi* through two complementary routes. First, unauthorised FX transfers may be pursued as

breaches of FX controls. Second, illegal transfers of funds into or out of the country may be treated as ML. This approach avoids the need for a standalone "underground banking" offence. Instead, it enables authorities to characterise HOSSP activity both as unauthorised financial service provision and as ML where funds are moved through illegal channels or for unauthorised purposes.

France addresses underground banking and HOSSP activity through existing offences rather than a specific "hawala" offence. Unlicensed MVTS, informal settlement networks, compensation mechanisms, and hawala-type arrangements may be treated as the illegal provision of banking or financial services when conducted without authorisation. France also relies on ML offences to address the movement and concealment of criminal value, particularly where transactions involve undeclared cash, opaque or circular settlement, lack of economic justification, or structures designed to conceal the source or destination of funds. A legal presumption of laundering may apply where transaction conditions are inconsistent with the lawful origin of assets, allowing prosecutors to proceed without proving the precise predicate offence where the circumstances indicate criminal origin.

154. Publicising sanctions is an important additional deterrent. An increasing number of jurisdictions not only sanction unauthorised operations but also make enforcement actions public, including regulatory warnings, sanctions, and, in some cases, conviction statistics. This strengthens deterrence and encourages compliance, particularly when combined with dissuasive penalties. It also supports international co-operation by informing other jurisdictions of emerging trends, typologies, and red flags, especially in cross-border PML cases. Such measures may include the regular publication of anonymised, disaggregated statistics on investigations, prosecutions, convictions, sanctions, and asset recoveries, with breakdowns—where possible—by channel (e.g. cash, TBML, VAs, PSPs, DNFBPs), sector, and corridor.

13. Extending underground banking and HOSSP controls to DNFBPs and key sectors

155. While underground banking and HOSSPs have traditionally relied on interaction with the regulated financial sector for transaction settlement, designated non-financial businesses and professions (DNFBP), sectors—particularly those providing professional services—may also play a significant role in facilitating PML schemes. Professional money launderers are diverse and often include legal professionals (such as lawyers and notaries), financial intermediaries (including accountants and financial advisers), and individuals operating informal networks. These professionals may provide the technical expertise required to design and operate complex legal, corporate, and transactional structures used to launder illicit proceeds, often in exchange for substantial fees.

156. In this context, extending underground banking and HOSSP-related controls, risk awareness, and supervisory focus to DNFBPs and key enabling sectors is encouraged, particularly those that facilitate or sustain complex ML arrangements. Strengthening sectoral understanding of underground banking and HOSSP typologies and embedding relevant controls within DNFBP supervision can reduce vulnerabilities and limit the ability of professional money launderers to exploit these sectors as facilitators or settlement channels.

157. At the same time, several sectors that are highly relevant to PML involving underground banking and HOSSPs—because they are frequently used as front businesses or settlement channels—do not fall within the FATF definition of DNFBPs. These include, for example, currency exchange shops, VASPs, and online lenders, which may instead be subject to AML/CFT obligations as FIs under the FATF Standards. Other sectors, such as import/export firms and travel agencies, may fall outside both the DNFBP and FI categories. In such cases, effective mitigation may nonetheless be achieved through close co-ordination with law enforcement and other competent authorities, including through oversight and information-sharing mechanisms related to tax, customs or trade-based controls.

14. Shifting from transaction-based enforcement to system-wide disruption of PML chains

158. This good practice reflects a strategic shift in addressing the use of underground banking and HOSSPs for PML. Rather than relying primarily on transaction-based or case-by-case enforcement, it promotes an end-to-end, system-wide approach aimed at disrupting the full architecture of underground banking and HOSSP-based PML schemes. In this context, scoping is important both for operational responses and for understanding the full transnational PML network.

159. A system-wide disruption approach involves:

(i) Mapping the full ML chain, by identifying each stage at which underground banking and HOSSP-related PML occurs (e.g. client recruitment, cash collection, settlement, trade mis-invoicing, and cash-out);

(ii) Applying targeted barriers at each stage, by assigning preventive and enforcement measures to all relevant actors, with clearly defined institutional responsibilities across FIUs, LEAs, central banks, supervisors, and tax and customs authorities; and

(iii) Deploying early disruption tools, including rapid restraint, freezing, and civil asset-recovery powers, to disrupt suspected HOSSP networks at an early stage, even where criminal prosecution is still under development.

160. Taken together, these elements form a "barrier model" that can be embedded within national AML strategies and multi-agency task force mandates. Beyond its analytical value, the model provides a structural co-ordination framework for operational action. Concrete measures may include licensing and authorisation checks, targeted inspections, labour and immigration controls, and tax audits, applied in a co-ordinated manner across the system.

Box 15. Barrier models and early disruption tools to target underground banking and HOSSP-based PML

Belgium: Belgian LEAs, with input from FIU Belgium, developed a "barrier model" to identify intervention points across the full ML chain involving underground banking and HOSSPs. The model maps the main stages of the laundering process, from cash generation and collection to value transfer, settlement, and reintegration. It identifies relevant actors, including predicate offenders,

professional money launderers, underground bankers, shell companies, cash couriers, false-invoicing networks, and trade intermediaries. It also highlights enabling conditions, such as sectoral vulnerabilities, regulatory gaps, and cross-border asymmetries. For each stage, the model defines targeted barriers and assigns them to competent authorities. These barriers may include identification measures, financial intelligence analysis, inspections, transaction monitoring, investigations, asset tracing, and domestic or international co-operation.

France: France has developed "short-track" procedures to enable the rapid freezing, seizure, and potential confiscation of funds held by short-lived shell companies suspected of being used for ML. The mechanism targets a key interface between underground banking or HOSSP networks and the formal financial system: bank accounts used by ephemeral companies to receive, move, or integrate illicit funds. Where objective indicators support a presumption of ML, FIU France may temporarily block debits from an account and alert the prosecutor. The prosecutor can then seek judicial confirmation of seizure without waiting for a full investigation to be completed.

161. More broadly, system-wide disruption of underground banking and HOSSP-based PML also requires a system-wide holistic approach. This entails proactively examining all major predicate crime investigations—particularly those involving fraud, online scams, gambling, migrant labour exploitation, and counterfeit goods—for underlying underground banking or HOSSP components. This represents a broader cultural shift that remains unevenly embedded within investigative services: any investigation into organised crime should systematically include a financial dimension focused on the laundering mechanisms used to process criminal proceeds. This financial focus is distinct from asset-tracing conducted for confiscation purposes and is intended to identify, disrupt, and dismantle the laundering infrastructure itself.

15. Establishing dedicated domestic co-ordination frameworks

162. This set of good practices addresses how jurisdictions organise themselves domestically to counter PML involving underground banking and HOSSPs. It focuses on institutional co-ordination models that align FIUs, LEAs, supervisors, prosecution services, sectoral authorities and, where relevant, private-sector partners around shared underground banking and HOSSP-related PML risks.

163. Effective action against underground banking and HOSSPs is strongly supported by robust domestic co-ordination mechanisms. National co-ordination committees, inter-agency task forces, standing committees, working groups, ad hoc task forces or national AML/CFT roundtables can play a critical role in prioritising underground banking and HOSSP-related risks, centralising information and financial intelligence, aligning enforcement priorities, sharing analytical outputs, and supporting the development of studies and typologies. Such mechanisms typically bring together supervisors, FIUs, LEAs, prosecutors, central banks, customs authorities, tax authorities, and security services.

164. Domestic co-ordination is most effective when underpinned by clear legal frameworks defining the status and criminalisation of underground banking activities. Legal clarity reduces ambiguity as to whether specific arrangements are illicit, thereby strengthening detection, inter-agency co-operation and enforcement.

165. Institutional co-ordination is further reinforced through joint training programmes, workshops and knowledge-sharing forums, which help establish a shared operational understanding across competent authorities, improve the quality and effective use of financial intelligence, and strengthen authorities' capacity to identify, investigate and respond to complex PML schemes involving underground banking and HOSSPs. Survey responses indicate that several jurisdictions have already implemented dedicated training initiatives explicitly focused on underground banking and HOSSP typologies, delivered in multi-agency formats bringing together FIUs, LEAs, supervisors, and prosecutors.

166. Building effective domestic co-ordination frameworks may also require evolving or expanding the role of certain competent authorities**.** For example, the mandate of tax administrations need not be confined to tax audits and revenue collection. Their detection tools and datasets can be leveraged for AML/CFT purposes, such as through the systematic cross-checking of annual corporate tax returns with monthly VAT transaction data, to identify anomalies indicative of underground banking or PML activity.

Box 16. Establishment of dedicated policy, institutional, and operational frameworks to address underground banking and HOSSP-based PML through co-ordinated action

The Netherlands characterises underground banking as informal value-transfer systems that may have originated from hawala-type arrangements but are now predominantly used to facilitate organised crime, particularly drug trafficking. Authorities consider that these systems have evolved to include currency trading with criminal funds and credit provision to criminal organisations. Given differences in criminalisation, legal rationale, and structure, Dutch authorities emphasise the importance of distinguishing underground banking, which involves laundering criminal proceeds, from HOSSPs, which may involve unlicensed services using licit funds.

In 2021, the Netherlands established a dedicated Taskforce Underground Banking as a joint multi-year initiative of the National Public Prosecutor's Office and the National Investigation Services of the Dutch Police. The taskforce targets professional informal value-transfer systems operating in or through the Netherlands, with a focus on disrupting networks, monitoring successor structures and emerging methods, and reducing criminal access to underground banking capacity. The taskforce combines prosecutorial, police, financial, digital, intelligence, and international co-operation expertise. It co-ordinates investigations, supports domestic and foreign partners, and helps determine which jurisdiction is best placed to act against cross-border networks or targets.

16. Detecting underground banking and HOSSPs and developing actionable intelligence across public and private sectors

167. These good practices relate to the detection of underground banking and HOSSPs, and to the development of actionable intelligence by combining: the establishment of formal feedback loops between competent authorities and reporting

entities; the development of targeted public–private partnerships (PPPs); the expansion of detection efforts beyond traditional supervisory and investigative tools; the establishment of public outreach and reporting channels; and the systematic consideration of intersections between underground banking/HOSSPs and the formal financial system.

16.1. Formal feedback loops between competent authorities and reporting entities

168. To enhance detection and intelligence development, competent authorities may establish formal, structured feedback mechanisms to systematically share underground banking and HOSSP-related typologies, red flags, and case outcomes with reporting entities, while collecting feedback on detection challenges, false positives, and operational constraints to refine indicators and monitoring approaches.

169. Structured, recurring feedback loops are a key enabler of effective detection and intelligence development in relation to underground banking and HOSSP-enabled PML. Such mechanisms are most effective when framed as a two-way, institutionalised function—rather than ad hoc engagement or one-off products—and when they operate on a repeatable basis to achieve three objectives:

(i) They systematically translate operational case experience into reusable detection content, including typologies, indicators, and red flags that reporting entities can operationalise in transaction monitoring and reporting.

(ii) They improve the quality and targeting of STRs/SARs through regular engagement formats (e.g. forums, working groups, or PPP channels) that allow competent authorities to communicate emerging threats and receive structured private-sector feedback on detection challenges, addressing the frequently cited lack of feedback. In this context, reporting entities—particularly banks—may be encouraged to analyse their micro-enterprise and SME customer portfolios operating in sensitive sectors (e.g. construction, private security, catering, small retail businesses) more granularly, including by developing sector-specific operating ratios and benchmarks based on their own customer data to support earlier identification of financial and management anomalies.

(iii) They create a virtuous cycle for intelligence development, whereby better-calibrated reports generate stronger FIU and LEA intelligence, which in turn informs refined indicators, typologies, and feedback to reporting entities—supporting progressively more effective detection, even where the core underground banking or HOSSP activity remains opaque.

170. Analysis of survey responses indicates that structured, recurring feedback mechanisms remain unevenly implemented. More targeted approaches may therefore be required.

16.2. Targeted public–private partnerships

171. Dedicated PPPs focused on underground banking and HOSSPs provide platforms not only for information sharing, but also for typology development, joint analysis, and targeted training beyond basic awareness-raising. Jurisdictions with dedicated PPPs report a range of operational benefits, including:

(i) Structured two-way intelligence exchange enabling the safe and lawful sharing of restricted information;

(ii) Identification of behavioural anomalies below STR thresholds, facilitating earlier network detection;

(iii) Improved quality and relevance of STRs and enhanced typology identification;

(iv) Near-real-time information exchange supporting more agile operational responses;

(v) Regular dialogue on indicators and red flags, including refinement of monitoring algorithms;

(vi) Joint analytical outputs derived from combined public- and private-sector data;

(vii) Integrated intelligence development, reducing fragmentation across authorities and sectors. Such collaboration is increasingly important given that FIs and other private-sector entities are often the first to identify suspicious activity linked to underground banking- and HOSSP-related PML.

172. Several jurisdictions shared examples of co-operation between authorities and private-sector stakeholders—such as FIs, compliance officers, and industry groups—to address these risks. This includes joint advisory groups, outreach programmes to regulated entities, as well as workshops and trainings for compliance officers.

Box 17. Targeted PPPs to enhance detection and intelligence development against underground banking and HOSSP-related PML

Germany's Anti Financial Crime Alliance uses public–private co-operation to strengthen detection of informal MVTS, underground banking, and HOSSP-related PML. Within this framework, AFCA published a typology-focused white paper on "hawala banking". The paper consolidates input from public authorities and private-sector obliged entities, including operational case studies, risk indicators, and analytical insights. It covers misuse of informal value-transfer systems for underground banking, TF, sanctions circumvention, and PML. The paper supports earlier detection and a shared understanding of complex, underground banking and HOSSP-based PML typologies.

16.3. Public outreach and reporting channels

173. Further enhancing detection and intelligence development entails establishing public outreach and reporting channels to encourage the reporting of suspected illegal underground banking and HOSSP activity. Measures reported include public registries, online portals, and whistle-blower channels that enable the verification of authorised remittance providers and facilitate the reporting of illegal operators; public education and awareness-raising initiatives, including warnings and sanctions publicity; and public alerts issued following NRA findings on underground banking and HOSSP-related risks.

174. Across jurisdictions, such outreach and reporting channels take diverse forms—ranging from whistle-blower hotlines and public registries to sanctions publicity and social-media monitoring—but serve a common function of broadening the detection surface beyond regulated entities and enabling the early identification of illegal underground banking and HOSSP activity. These mechanisms are most effective when combined with clear public messaging on authorisation requirements, visible enforcement outcomes, and effective integration with supervisory and law-enforcement workflows.

Box 18. Public outreach and reporting channels to detect illegal underground banking and HOSSP activity

United Kingdom: In the UK, public-facing guidance, enforcement warnings, and reporting channels support the detection of illegal HOSSPs and underground banking operators. Authorities may also identify suspected unlicensed activity through publicly visible online advertising for informal remittance services. Publicity around sanctions and asset recovery actions can further encourage reporting and reduce the perceived impunity of illegal operators.

16.4. Detection beyond 'traditional' tools

175. Detection and intelligence development may be further strengthened by extending efforts beyond traditional supervisory and investigative tools. This includes enabling supervisors to deploy specialised techniques—such as mystery shopping or agent-based approaches—to identify unlicensed MVTS, underground banking operations, and HOSSPs, as well as promoting open-source intelligence (OSINT) and social-media monitoring as standard detection tools. Underground banking operators, HOSSPs, and PML actors increasingly rely on social-media platforms for client acquisition, communication, and the recruitment of intermediaries. Their growing use of open, semi-closed, and encrypted online environments underscores the need to complement traditional approaches with digitally focused detection capabilities. When embedded in routine supervisory and enforcement processes and supported by inter-agency co-operation, such digital tools can significantly enhance the detection of underground banking and HOSSP-related PML activity.

176. This requires the development of specialised capacity across competent authorities. Targeted training for supervisors, FIUs, LEAs, and prosecutors on underground banking and HOSSP typologies, digital forensics, and VA tracing supports the analysis of complex behavioural and transactional patterns, the development of credible red-flag indicators, and the maintenance of up-to-date typologies aligned with evolving digital risks.

177. Cultural intelligence capabilities (see Box 19) are also critical to understanding the phenomena described in this report. As investigations focus on the financial dimension (see subsection 15), incorporating the cultural dimension contributes to a more holistic approach to disrupting the full architecture of underground banking and HOSSP-based PML schemes.

178. Capacity-building efforts may further include the development of methodological playbooks and operational guidance. While approximately half of jurisdictions report some training on underground banking and HOSSPs, only around one-third provide training specifically focused on PML through these channels. General or overly broad programmes are therefore unlikely to support effective detection or disruption without dedicated, risk-specific content that integrates both traditional and digital detection approaches.

Box 19. Detection beyond 'traditional tools'

Europol: What is cultural intelligence?

Cultural intelligence (CULINT) is a crucial tool for tackling the use of underground banking and HOSSPs for PML. This approach recognises the importance of understanding the cultural dimensions and social networks that underpin these illicit activities. By leveraging cultural intelligence, FIUs and LEAs can better penetrate the tightly-knit communities often involved in underground banking. This understanding helps in identifying key players, deciphering complex transaction patterns, and developing more effective investigative strategies. Cultural intelligence enables investigators to navigate the nuances of different cultural practices, enhancing their ability to detect and disrupt sophisticated PML networks.

Oman: OSINT and social-media monitoring to detect underground banking and HOSSP-related activity

Oman uses OSINT and social-media monitoring to detect underground banking, unlicensed MVTS, and HOSSP-related activity. Authorities monitor online advertisements, referrals, and discussions promoting informal remittance or hawala-type services, including content directed at specific communities and activity taking place through social media, closed groups, or encrypted messaging applications. The Central Bank of Oman combines these outputs with whistle-blower reports, supervisory intelligence, data from supervised entities, law enforcement feedback, and analysis of banking and remittance indicators to identify high-risk cases, support referrals to the FIU and law enforcement, and inform enforcement action. Oman also applies automated monitoring and trend analysis, informed by developments observed across the financial sector and payment industry. This uses incremental tools rather than full-scale machine-learning models to detect emerging typologies, including shifts from cash-based hawala to e-wallets and other digital payment methods.

16.5. Intersections between underground banking/HOSSPs and the formal financial system

179. Finally, jurisdictions may strengthen detection by systematically considering intersections between underground banking/HOSSPs and the formal financial system, and by leveraging the formal financial layer as a detection surface. While informal MVTS operate outside regulatory frameworks, their interaction with regulated FIs and products creates opportunities for both exploitation and detection. Professional money launderers strategically target weaker elements of the formal

financial sector to facilitate underground banking activity, using regulated accounts, corporate structures, and investments to manage or move proceeds of crime. In some cases, actors have shifted from formal channels to underground methods in response to increased scrutiny or de-risking. These dynamics underscore the importance of integrated approaches among supervisors, FIUs, and LEAs to map and analyse interfaces between underground banking networks, HOSSPs, and regulated entities. Key nodes at this interface include vIBANs, PSPs, fintech platforms, and other digital payment solutions, which may function as gateways or enablers for underground flows and blur the boundary between licit and illicit financial activity.

Box 20. Leveraging the interface between underground banking/HOSSPs and the formal financial system for detection of underground banking and HOSSP-based schemes

Luxembourg uses information from the regulated financial sector and its wider service ecosystem to detect unauthorised underground banking, HOSSPs, and other unlicensed financial activity. The supervisory authority draws on reports from regulated entities and service providers, whistle-blower information, complaints, domestic authorities, foreign supervisory warnings, open-source checks, and company registry cross-checks. Suspicious transaction and activity reports to the FIU also help identify patterns linked to unauthorised HOSSPs or underground banking. For VA activity, detection is supported by media monitoring, public sources, supervisor–FIU information exchange, and targeted information requests to clarify whether operators are authorised. Where unauthorised activity is identified, warnings may be published and cases referred to prosecutors.

17. Maintaining centralised data and assessing risk

180. The following good practices emphasise the maintenance of centralised statistics and case registries on underground banking and HOSSPs, and the systematic integration of their ML/TF risks into NRAs and sectoral risk assessments, in order to support targeted policy, supervisory, and enforcement actions. Centralised data collection and risk analysis enable jurisdictions to address the opacity of these systems, strengthen their understanding of PML typologies, and ensure that strategic risk assessments translate into intelligence-led supervision, investigations, and co-ordinated operational responses.

17.1. Maintaining centralised statistics and case registries

181. Maintaining centralised statistics and case registries on underground banking and HOSSPs can enhance a jurisdiction's capacity to detect these activities, allocate supervisory and enforcement resources, shape policy responses, and improve investigative outcomes. Such systems—typically hosted by the FIU or a central AML/CFT authority—can consolidate, through structured and standardised data collection, information on investigations, prosecutions, convictions, administrative actions, seizures and confiscations, as well as suspicious transaction report and suspicious activity report (STR/SAR) data linked to underground banking and HOSSP

typologies. Consolidated data supports a more comprehensive understanding of risk exposure and emerging trends.

182. Survey responses highlight the importance of structured, standardised reporting by competent authorities into these centralised systems. Consistent data submission enables the aggregation and analysis of enforcement, intelligence, and supervisory information. Outputs can inform NRAs, sectoral risk assessments, and compliance targeting, facilitating the translation of strategic risk analysis into more focused operational action. Data derived from investigations, sanctions, and STR trends can also be leveraged to generate actionable supervisory insights. Jurisdictions may therefore consider how centralised statistics and case registries on underground banking and HOSSPs can strengthen the operational impact of strategic assessments and overall AML/CFT effectiveness.

Box 21. Using centralised data, enforcement statistics, and supervisory insights to address underground banking and HOSSP risks

Malaysia uses centralised supervisory, enforcement, and financial intelligence data to identify and mitigate risks linked to illegal money service businesses, including unlicensed MVTS and HOSSP-related activity. Bank Negara Malaysia consolidates information from multiple sources, including STRs, CTRs, public complaints, supervisory data, enforcement outcomes, and targeted detection techniques such as mystery shopping. This data-driven approach helps identify illicit remittance patterns, and map unlicensed operators. The information is used to guide joint action with law enforcement and other competent authorities, including investigations and prosecutions. Enforcement results are also recorded and analysed to identify trends, inform risk assessment, and support supervisory prioritisation. BNM also publishes all enforcement actions on its website, including those involving HOSSP-equivalent activity, reinforcing transparency and deterrence.

17.2. Embedding underground banking and HOSSPs as distinct components of NRAs

183. A majority of jurisdictions report having assessed ML, TF, and proliferation financing (PF) risks associated with underground banking and HOSSPs, most commonly through their NRAs. Jurisdictions that have not undertaken such assessments are predominantly smaller or lower-capacity jurisdictions, highlighting the inclusion of these risks as an indicator of AML/CFT system maturity.

184. Among jurisdictions that have conducted risk assessments, underground banking and HOSSPs are most often identified as presenting a high risk of abuse for ML and/or TF. Approximately one third of jurisdictions explicitly recognise PML within their NRAs and link underground banking and HOSSPs to key predicate offences (see subsection 8.1.). Accordingly, in jurisdictions where such predicate offences are prevalent, their existence may in itself trigger a risk diagnosis encompassing underground banking- and HOSSP-based PML schemes.

185. In this context, it is considered good practice for jurisdictions to treat underground banking and HOSSPs systematically and at a granular level as distinct or stand-alone risk areas within national risk frameworks, rather than subsuming them

under broader or generic MVTS categories. This approach enables a clearer articulation of threats, vulnerabilities, and consequences, and supports the development of more targeted and proportionate mitigation measures. NRAs may also assess both domestic exposure and a jurisdiction's potential role as a hub or transit point within global underground banking- and HOSSP-based PML networks (see subsection 9.2.4.). Explicit identification of these systems allows jurisdictions to better assess where and how they operate, the predicate offences to which they are most commonly linked, and the ways in which they may be exploited by professional money launderers. Such analytical clarity is essential for accurate risk diagnosis and for the design of effective policy, supervisory, and enforcement responses.

186. In addition to NRAs with dedicated chapters, jurisdictions have also assessed ML/TF risks related to underground banking and HOSSPs through stand-alone or sector-specific risk assessments, including intelligence-driven reviews linked to PML typologies.

187. For the purposes of this report, a sectoral risk assessment refers to a targeted, risk-based analysis conducted by a jurisdiction to identify, assess, and understand ML, TF, and PF risks associated with specific categories of actors or activities exposed to underground banking systems and HOSSPs. Sectoral risk assessments may be conducted as stand-alone exercises or as part of a broader NRA, and typically focus on:

(i) Specific obliged professions or regulated sectors exposed to HOSSP misuse (such as MVTS, currency exchangers, PSPs, DNFBPs, and VASPs); and/or

(ii) Specific economic activity sectors presenting heightened vulnerability due to their operating characteristics, including construction and public works, private security, hospitality and catering, vehicle trade, import/export and trade-based sectors, informal or cash-intensive services, and, in some regions, ICT- or online-enabled services.

188. These sectors are not always sharply defined and are typically identified through typologies, case experience, or law-enforcement intelligence rather than rigid legal classifications. The objective of sectoral risk assessments is risk prioritisation rather than exhaustive classification.

Box 22. Embedding underground banking and HOSSPs as distinct components of NRAs

Italy explicitly incorporates underground banking and HOSSP-related risks into its NRA, with a focus on systemic vulnerabilities such as cash intensity, multi-intermediation, and cross-border financial structures, particularly where illicit payment services intersect with regulated sectors such as PSPs. The assessment draws on STRs, other reports and communications, as well as data from financial intermediaries and investigative findings to identify ML/TF trends, exposure points, and sectoral vulnerabilities. Italy also uses network-mapping tools, social network analysis, FIU-to-FIU co-operation, and co-ordination with supervisory and customs authorities to support a more granular understanding of HOSSP-related risks.

17.3. Linking NRA and sectoral risk assessment findings to concrete policy, supervisory, and enforcement action

189. NRAs and sectoral risk assessments can be used as operational tools to drive concrete policy, supervisory, and enforcement responses to PML risks associated with underground banking and HOSSPs. In particular, jurisdictions may use risk assessment findings to:

(i) Identify high-risk hubs (such as cities, border areas, and commercial districts), sectors (including money or value-transfer services and agent networks, FX dealers, and import–export firms), and corridors, and to reorient supervisory and enforcement priorities accordingly; and

(ii) Use published sanctions statistics to assess the effectiveness of policy measures and to guide the allocation of supervisory and enforcement resources.

190. Experience from several jurisdictions shows that translating NRA findings on underground banking and HOSSPs into tangible changes in policy, supervision, and institutional practices can significantly strengthen national responses to PML. Ensuring that NRA conclusions are systematically operationalised is therefore critical to preventing risks related to underground banking and HOSSPs from being overlooked and to reducing their attractiveness to PML networks.

Box 23. Translating NRA findings on HOSSP risks into supervisory and enforcement action

Germany's National Risk Assessment identified informal MVTS, particularly HOSSPs, as a significant ML/TF risk. Germany translated this finding into supervisory and enforcement priorities. MVTS operators require a BaFin licence, and unlicensed activity is prohibited and may constitute a criminal offence. Since 2019, the pursuit of unlicensed MVTS has been treated as a supervisory priority, supported by additional federal resources for enforcement. NRA findings, together with BaFin and FIU analysis, have also been converted into practical detection points. These include transactions involving unclear beneficial ownership, unknown sources of funds, unusual activity, third-party involvement, and links to higher-risk cross-border corridors.

18. Investigating and prosecuting

191. The following good practices focus on how cases involving the use of underground banking and HOSSPs for PML can be effectively investigated, prosecuted, and brought to court. They include:

(i) Using legal and procedural tools to address evidentiary challenges in PML cases, including legal mechanisms that ease evidentiary burdens in clearly defined circumstances consistent with due process. This may include legal presumptions of ML or illicit origin (see Box 14), streamlined asset-freezing and confiscation regimes applicable to underground banking and HOSSP-related offences (such as self-

laundering provisions and expanded confiscation powers), and the systematic use of financial intelligence in criminal proceedings and before courts;

(ii) Promoting specialised investigation and prosecution capacities, including dedicated financial crime or PML units where caseloads justify it, and the use of joint analytical and investigative teams at national, regional, and international levels to address underground banking and HOSSPs used for PML;

(iii) Leveraging advanced investigative techniques and technologies, including live electronic investigations, decryption capabilities, and other digital forensic tools relevant to complex, technology-enabled PML schemes; and

(iv) Developing specialised training for criminal justice practitioners, including tailored training modules for investigators, prosecutors, and judges, and the effective use of existing guidance and typologies on financial crime and PML.

Box 24. Legal and procedural tools, financial intelligence, and advanced investigative techniques in PML cases involving underground banking and HOSSPs

France reports a court-facing mechanism through which the FIU, Tracfin, may transmit relevant information directly to judicial authorities in support of investigations and proceedings. These transmissions may include bank account details in France or abroad, transaction data, financial links between natural or legal persons, and possible location indicators for persons involved. This mechanism helps ensure that financial intelligence supports not only initial detection, but also evidentiary development and procedural decision-making in ongoing cases.

Türkiye uses prosecutor-led criminal procedure powers to investigate complex ML cases involving underground banking and HOSSP-based schemes. These include interception and recording of communications, technical surveillance, access to computer systems and digital data, searches, seizure of evidence, and requests for records from obliged entities or other relevant persons. Undercover operations may also be used in ML/TF cases. On the administrative side, the Central Bank of the Republic of Türkiye supervises HOSSP activities, while MASAK analyses related STRs and disseminates findings to the Central Bank and prosecutors. Together, these tools help corroborate STRs and transaction analysis with communications, device evidence, and operational records. They are particularly relevant to technology-enabled "digital hawala" typologies, where they can help identify co-ordinators, facilitators, nominee structures, network roles, and cross-border links.

19. Deepening international co-operation

192. PML involving underground banking and HOSSPs is inherently transnational. Such schemes rely on cross-border fund flows and exploit informal MVTS, as well as legal and regulatory inconsistencies between jurisdictions, to obscure the origin, movement, and destination of illicit proceeds. Reflecting this reality, 90% of the

detailed case examples submitted by jurisdictions in the survey contained a cross-border element.

193. Jurisdictions emphasise that effective international co-operation in this area requires action across conceptual, legal, and practical dimensions.

194. At the conceptual and legal level, jurisdictions stress the need for greater cross-border alignment. Divergent legal definitions, regulatory treatment, and risk recognition of underground banking and HOSSPs remain significant impediments to co-operation. Where definitions, offences, or procedural rules differ, professional money launderers are able to exploit these gaps to evade detection and enforcement. A core good practice is therefore to promote greater harmonisation of legal concepts relating to underground banking and HOSSPs, including the alignment of offences covering unauthorised MVTS and PML. Enhanced legal alignment can reduce dual criminality obstacles and facilitate extradition, MLA, and joint investigations.

195. In parallel with legal harmonisation, jurisdictions identify a range of practical measures to strengthen international co-operation:

(i) Enhancing operational information sharing. Jurisdictions highlight the importance of improving the security, speed, and usability of information-sharing platforms, such as the Egmont Secure Web, to enable faster and more effective intelligence exchange. Good practices also include providing training and technical assistance to foreign counterparts to improve their capacity to respond to co-operation requests, as well as promoting and funding cross-border, multi-agency operations. Such operations are widely regarded as among the most effective tools for disrupting international criminal networks reliant on underground banking and HOSSPs.

(ii) Leveraging diverse co-operation tools and networks. Jurisdictions underscore the value of using a broad range of international co-operation frameworks, including international roundtables, practitioner groups, law enforcement networks, and multi-channel co-operation models that combine formal and informal mechanisms. International co-operation is particularly important for joint analytical work, including the region-specific refinement of typologies, red flags, and indicators related to underground banking and HOSSPs. Case study analysis demonstrates the effectiveness of informal co-operation—used either prior to or alongside formal MLA—especially in fast-moving and opaque PML schemes. This includes co-operation through networks such as INTERPOL, Europol, AMON, and the Five Eyes Law Enforcement Group, as well as direct bilateral exchanges. The effectiveness of these channels varies depending on the typology involved and the urgency of the investigation.

(iii) Engaging proactively with international partners. Effective co-operation depends on a willingness to engage constructively and proactively. A good practice is for jurisdictions that detect underground banking networks or HOSSP-based PML schemes to promptly inform relevant international counterparts. Early notification facilitates timely intelligence sharing, co-ordinated analysis, and, where appropriate, joint investigative or enforcement action.

(iv) Applying existing international guidance and operational feedback. The detection, investigation, and prosecution of PML schemes involving underground banking and HOSSPs raise specific cross-border challenges, including the time-sensitive nature of cases and the need for clear and

reliable channels for urgent information exchange. Jurisdictions note that these challenges can be addressed by leveraging established international guidance and operational feedback on international co-operation for AML/CFT purposes, including the methods set out in the 2025 FATF–Egmont Group–INTERPOL–UNODC handbook on international co-operation[18] and in the asset recovery guidance[19], and applying them to the specific risks posed by underground banking and HOSSP-related PML.

Box 25. Disrupting a '*Fei Ch'ien*' underground banking network through INTERPOL Purple Notice

Italy: In 2024, Italian authorities conducted 'Operation Fei Ch'ien' targeting an underground banking network used to launder proceeds from large-scale drug trafficking. The scheme involved two drug-trafficking groups and a separate PML group that provided 'flying money' services to multiple criminal clients. Criminal cash was collected through front businesses in the import-export sector, particularly clothing and fashion, which acted as covert cash collection hubs despite limited genuine activity. Transfers were linked to pre-agreed alphanumeric codes, allowing value to be moved anonymously while the PML network assumed the operational and legal risk. The settlement model evolved from courier-based cash smuggling to non-physical mechanisms, including fictitious trade transactions, multi-jurisdictional financial triangulation, and internal offsetting. Given the network's transnational relevance, Guardia di Finanza issued an INTERPOL Purple Notice to raise awareness on this modus operandi with other jurisdictions, so that the appropriate preventive and precautionary measures can be taken. This helped support international detection and co-ordinated action against similar underground banking and HOSSP-based PML networks.

20. Leveraging technology, innovation, and digital infrastructure

196. To combat the use of underground banking and HOSSPs for PML, jurisdictions increasingly rely on a combination of technological tools, digital infrastructure, and enabling legal frameworks. Good practices in this area focus on leveraging technology, advanced analytics, and integrated data environments to address the growing digitalisation and hybridisation of underground banking systems. This includes investing in advanced technological capabilities and establishing the legal foundations necessary for their effective use by competent authorities.

Technological innovation is a structural driver of the evolution of underground banking and HOSSPs and therefore necessitates technology-intensive countermeasures. Traditional supervisory and investigative approaches are increasingly insufficient to address the scale, speed and complexity of digitally

[18] FATF – Egmont Group – INTERPOL – UNODC (2025), *International Co-operation on Money Laundering Detection, Investigation, and Prosecution Handbook*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/International-Co-operation-ML-Detection-Investigation-Prosecution.pdf.coredownload.pdf

[19] FATF (2025), *Asset Recovery Guidance and Best Practices*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Asset-Recovery-Guidance-Best-Practices.pdf.coredownload.pdf

enabled and hybrid schemes. Notably, fragmented data environments significantly constrain the ability of competent authorities to detect and respond to multi-channel laundering activities. While the use of data analytics is expanding, adoption remains uneven across jurisdictions, with the most advanced capabilities typically observed in jurisdictions with mature FIUs and structured PPPs.

197. To keep pace with evolving typologies, jurisdictions increasingly recognise the need for innovative, technology-enabled approaches, including advanced analytics and AI. The integration of traditional underground banking and HOSSP networks with modern technologies – such as encrypted communication tools, VAs, PSPs, e-commerce platforms and mobile money – reinforces the need for integrated digital infrastructures capable of consolidating and analysing data across multiple sectors, platforms and payment rails. This requires moving beyond siloed supervisory and investigative tools towards more holistic, cross-cutting analytical capabilities.

198. In this context, the technology-driven good practices include:

(i) **Integrated, cross-sector and multi-agency digital infrastructure.** Developing integrated digital infrastructures that link supervisors, FIUs, law enforcement authorities and, where appropriate, customs and tax authorities enables the aggregation and analysis of information from diverse sources. These may include data from regulated FIs, VASPs, PSPs, and relevant public or private registries. Interoperable systems – such as shared analytical platforms and co-ordinated access to financial, VA, and payment-system data – support pattern recognition across otherwise disconnected datasets, enhancing the detection of underground banking and HOSSP-related activity spanning both formal and informal channels.

(ii) **Advanced analytics for risk prioritisation.** The use of machine-learning-based scoring modules to prioritise STRs potentially linked to underground banking or HOSSP activity can improve the efficiency and effectiveness of analytical processes, particularly in high-volume reporting environments.

199. Jurisdictions emphasise, however, that legal and practical constraints must be addressed to enable the effective deployment of such technologies. Legal obstacles—particularly those related to personal data protection—as well as budgetary constraints, given the high cost of advanced IT tools in resource-constrained environments (notably lower-capacity jurisdictions), should not be underestimated and must be anticipated at an early stage.

Box 26. Technological approaches to detecting and disrupting underground banking and HOSSP-related PML

Indonesia's FIU, PPATK, uses blockchain analytics tools to trace VA flows where unauthorised MVTS and HOSSP-related schemes intersect with VAs. These tools help follow peer-to-peer VA transactions used to settle value between HOSSP operators, particularly in fraud and online scam cases. The tracing results are integrated into financial intelligence analysis and shared with law enforcement to support investigations into hybrid cash–VA ML schemes.

Nigeria uses the goAML platform to receive and conduct initial analysis of STRs, including reports linked to underground banking and informal FX activity. The Nigerian FIU applies risk-based analytics to prioritise STRs involving unlicensed

money changers, hawaladars and cash-intensive intermediaries. Relevant STRs are converted into actionable intelligence reports, using additional data integrated into the NFIU's analytical processes, including BOI data, trade data from Customs as well as tax data, and shared with law enforcement and supervisory authorities, through the secure CRIMS platform. Relevant STRs are converted into actionable intelligence reports and shared with law enforcement and supervisory authorities, including the Central Bank of Nigeria and the Economic and Financial Crimes Commission, through the secure CRIMS platform. This workflow supports case identification, investigation, prosecution and asset freezing.

21. Promoting financial inclusion

200. The following points set out good practices for promoting financial inclusion as a means of reducing reliance on illegal underground banking and HOSSPs, while mitigating the risks of PML and the unintended impacts of measures to combat the use of underground banking and HOSSPs for PML.

201. Jurisdictions emphasise that AML/CFT frameworks should be implemented in a manner consistent with national financial inclusion strategies, where such strategies exist. Authorities recognise that the use of underground banking and HOSSPs is not, in itself, indicative of ML or TF. In a range of contexts—including cash courier arrangements, small-value trade-related payments, and remittance corridors serving fragile or conflict-affected regions—such mechanisms may facilitate licit economic activity where access to formal banking services is limited, costly or unavailable. Similarly, underground banking and HOSSPs may meet legitimate financial needs of migrants, refugees, and diaspora communities originating from jurisdictions with underdeveloped or non-existent banking infrastructure.

202. Against this backdrop, jurisdictions highlight the importance of calibrated enforcement approaches that distinguish between organised criminal exploitation of underground banking and HOSSPs and individual users seeking to meet legitimate financial needs. Overly punitive or indiscriminate enforcement measures may inadvertently increase financial exclusion, undermine trust in authorities, and displace legitimate users further towards unregulated channels, thereby increasing ML and PML vulnerabilities. At the same time, jurisdictions also note that uneven regulatory frameworks and enforcement, as well as fragmentation between regulatory regimes, may perpetuate underground banking and HOSSP techniques and support their development.

203. Many jurisdictions therefore view financial inclusion as a risk mitigation strategy within their AML/CFT frameworks. When designed with appropriate safeguards, measures aimed at expanding access to safe, affordable, and efficient formal financial services—such as digital payment platforms, lower-cost remittance products, tiered CDD, and simplified onboarding processes—can reduce demand for illegal underground banking and HOSSPs while enhancing transparency and traceability. Jurisdictions further note that de-risking by major banks, including the termination of correspondent banking relationships with high-risk jurisdictions, has contributed to some transactions migrating towards MVTS, both licensed and unlicensed—a trend viewed critically by law enforcement given that unlicensed transfers are extremely difficult to trace and can hinder investigations.

204. Effective enforcement may be complemented by targeted initiatives designed to reduce financial crime risks faced by remittance-dependent and cash-reliant communities. Jurisdictions underscore the value of community-based education and outreach initiatives, particularly those addressing fraud risks, misuse of informal channels, and indicators of PML activity. Such initiatives are often prioritised for migrant workers, diaspora communities, and other populations exhibiting higher reliance on MVTS, and may involve multi-language materials and culturally appropriate messaging.

205. Constructive engagement with affected communities and sectors is a recurring theme across jurisdictions. Authorities report positive outcomes from collaborating with diaspora leaders, employers, labour organisations, and community groups to co-design outreach campaigns and encourage the use of authorised and supervised channels. This engagement may be supported through dedicated working groups focusing on cash wages, migrant labour, cash-intensive industries, informal payment practices, and remittance corridors, as well as regular conferences and outreach events where typologies and risks related to PML, underground banking, and HOSSPs are shared with relevant stakeholders.

206. PPPs and broader sectoral engagement further support these objectives. Jurisdictions note the benefits of collaboration between competent authorities, FIs, authorised MVTS providers, fintech firms, and civil society organisations to build capacity, share information, and develop a collective understanding of risks and mitigation strategies. Such partnerships can help align compliance requirements with financial inclusion objectives, reduce unintended barriers to access, and strengthen the detection of criminal abuse.

207. Jurisdictions also highlight the importance of integrating these complementary approaches into NRAs and national AML/CFT strategies. Reflecting financial inclusion considerations in risk assessments, policy development, and enforcement priorities can help ensure that measures to address PML risks do not inadvertently exacerbate financial exclusion or undermine legitimate economic activity.

208. Overall, case studies demonstrate that combining targeted enforcement against organised criminal exploitation with proportionate financial inclusion measures can effectively mitigate PML risks, while avoiding the displacement of legitimate users towards illegal underground banking and HOSSPs.

Box 27. Financial inclusion as a tool to mitigate PML risks

Indonesia uses financial inclusion measures to help reduce reliance on informal value transfer-channels, including hawala-type systems and unlicensed money changers. The approach combines public awareness, financial literacy, and proportionate regulation. Awareness campaigns help users understand the risks of informal channels, while financial literacy initiatives promote the benefits of regulated services. Regulatory measures aim to keep formal remittance channels accessible and cost-effective, reducing incentives for customers to move to underground or offshore alternatives. The practice illustrates how financial inclusion can complement enforcement by reducing demand for informal HOSSP

channels, particularly in contexts with significant migrant communities and cross-border remittance flows.

Portugal combines enforcement against unlicensed MVTS with public communication aimed at reducing reliance on informal value-transfer channels. Banco de Portugal issues public warnings and provides information on authorised providers and the risks of using unlicensed operators. Awareness-raising is targeted at users who may depend on remittance services or may be unaware that certain informal services are illegal. Dissemination through media channels helps extend the preventive effect. The approach also raises awareness among FIs, supporting stronger internal controls and improved reporting of HOSSP-type arrangements. The practice illustrates how financial inclusion and awareness measures can complement enforcement by steering users toward regulated channels, reducing demand for informal services, and improving detection by reporting entities.

Report definitions

Cash courier

Individual who physically transports cash or bearer negotiable instruments on behalf of others, often across borders, to rebalance positions between service providers.

Compensation

A settlement mechanism by which underground banking operators or HOSSPs do not transfer funds for each individual transaction, but instead offset reciprocal obligations and settle only the net amount owed after a period of time.

Hawala and other similar service providers

A subset of money or value-transfer services that arrange the transfer and receipt of funds or equivalent value and settle through non-bank mechanisms such as trade, cash, and net settlement over extended periods. Their defining structural feature is reliance on informal compensation mechanisms, although they may also use formal financial channels as part of hybrid settlement arrangements. Their use is not inherently criminal and may serve legitimate remittance and value-transfer needs, but they may also be exploited or misused for illicit financial activity. The provision of unregistered HOSSP services is generally a criminal offence in most countries.

International controller network

For the purposes of this report, a cross-border PML network, often operating through underground banking and/or HOSSP mechanisms, TBML, bulk cash movement and VAs, in which one or more controllers—consistent with the controller role described in the 2013 FATF report[20]—arrange, direct, or oversee the collection, movement, settlement, and delivery of criminal value across multiple jurisdictions. Such networks may involve

[20] FATF (2013), *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Role-of-hawala-and-similar-in-ml-tf.pdf. See also subsection 5.3. of this report.

collectors, co-ordinators, transmitters, correspondent brokers, complicit businesses, and other settlement mechanisms, and may form part of broader PML schemes..

Money mule

Person who transfers, moves, deposits, withdraws, or converts criminal proceeds on behalf of another person or criminal network, typically through their own financial accounts or financial instruments, thereby obscuring the origin and ownership of the funds.

Money service business

Business that offers financial services centered on the movement, exchange, or conversion of funds or value, including, as applicable under domestic law, money transmission, FX, cheque cashing, and the issuance or redemption of payment instruments or stored value.

Money or value-transfer services

Financial services involving the acceptance of cash, cheques, other monetary instruments, or other stores of value, and the payment of a corresponding sum to a beneficiary by communication, message, transfer, or through a clearing network to which the provider belongs. The transaction may involve intermediaries, a final payment to a third party, and may include new payment methods.

Professional money laundering

The laundering of criminal proceeds by individuals, organisations, or networks that specialise in providing money laundering services to criminals and engage in third-party laundering for a fee or commission. These actors help criminals launder the proceeds of illegal activity and are typically separate from the underlying proceeds-generating crime.

Underground banking

Informal arrangements that operate outside, alongside, or through the regulated financial system and enable the transfer, settlement, or storage of value through networks of intermediaries. Such arrangements may rely on compensation mechanisms, and may include HOSSPs, but may also employ a broader range of mechanisms. Underground banking is not inherently criminal and may be used to transfer both licit and illicit funds, though it presents elevated ML and TF risks because of limited transparency, weak or non-existent record-keeping, reliance on informal settlement mechanisms, and, in some cases, operation outside licensing, registration, or supervisory frameworks.

Third party payment

A transfer of funds made by, to, or through a third party rather than directly between the principal parties to the underlying transaction, often as a settlement method. In the underground banking and HOSSP-based professional money laundering context, such payments can be used to move excess value, obscure transactional links, and facilitate fraud or laundering schemes, including through invoice settlement.

Token

In the context of criminal transfers conducted through underground banking and HOSSPs, a simple authentication and control mechanism used to ensure that cash is paid out to the intended recipient and to evidence that a handover has occurred. Tokens most commonly take the form of a unique serial number on a banknote, which is communicated through the transfer chain and must be produced or matched at the point of collection, thereby providing a basic form of identification and a rudimentary receipt.

Compilation of additional case studies and good practices examples

5. Role of underground banking and HOSSPs in PML

Box 28. Use of underground banking systems and HOSSP-based PML schemes in drug trafficking

Europol: Operation Whitewall was launched by the Spanish Guardia Civil in early 2021 following the seizure of cocaine and large amounts of cash from vehicles fitted with hidden compartments. Some of the seized banknotes bore handwritten inscriptions, or 'tokens', which appeared to identify those co-ordinating the financial side of the drug-trafficking activity. Analysis of encrypted communications from EncroChat and Sky ECC, supported by Europol and partner countries, helped identify a high-value target operating a parallel financial system from Spain. The individual provided PML services to multiple organised crime groups, including drug-trafficking networks, by arranging cash pick-ups across Europe and the delivery or settlement of equivalent value in other jurisdictions. The network used a combination of underground banking and HOSSP-related techniques, including hawala-style settlement, bulk cash smuggling, misuse of legal business structures, shell companies, front men, luxury goods and vehicles, and real estate investment.

United Kingdom: A 2020 drug-trafficking investigation identified the use of trade-based settlement within an ICN. Drug proceeds collected in cash in the UK were exchanged for equivalent value in euros in the Netherlands and other jurisdictions, including to finance further drug shipments. The cash was consolidated in a safe house, counted and reconciled, and then moved through complicit money service businesses. These MSBs disguised the funds in their records as multiple low-value remittances to Afghanistan and other destinations. The funds were then channelled through a wholesale MSB with access to banking facilities and transferred, on instruction, to Chinese businesses or exchange houses in the United Arab Emirates (UAE). The scheme used criminal cash to settle genuine trade debts, including payments for goods imported from China into Afghanistan and other jurisdictions. This allowed the controller network to convert UK drug proceeds into apparently legitimate trade settlement value, while traders benefited from off-book payments and the undervaluation of imported goods.

Box 29. Illegal online gambling proceeds laundered through HOSSP-based networks

India: Indian authorities identified a PML scheme linked to an illegal online gambling platform that generated proceeds from sports betting, card games, and other forms of online wagering. The platform relied on a decentralised network of "panel operators" to manage customer deposits and withdrawals. These operators used UPI, online banking, digital wallets, mule accounts, and accounts opened with stolen identities to receive and move funds. The structure enabled the organisers

to separate the gambling platform from the financial flows supporting it. A portion of the proceeds was converted into cash and moved abroad through hawala and other underground banking channels. Funds were then reintroduced into India as purported foreign investment from the UAE, disguising the criminal origin of the proceeds.

6. Settlement methods

Box 30. VA-based settlements in underground banking and HOSSP-based PML

Japan: Japanese authorities identified underground banking schemes in which operators collected cash or bank deposits in Japan and converted the funds into VAs. The VAs were then transferred to wallets in foreign jurisdictions, where counterpart operators converted them into stablecoins, such as USDT, or local fiat currency before paying the intended beneficiary. In this model, VAs functioned as a settlement layer between underground banking operators. The domestic operator aggregated value in Japan and transmitted it internationally through blockchain transfers, while the foreign counterpart completed the local payout. This enabled cross-border value transfer without moving cash or bank transfers directly across borders. The schemes were supported by mule accounts, accounts held in false or third-party names, unregistered VA exchange activity, and non-face-to-face communication through social media or encrypted messaging applications.

7. Emerging typologies and trends

Box 31. Hybrid settlement models combining VAs and precious metals and stones

Oman: Omani authorities identified underground banking and HOSSP-style schemes that combined cash, mobile money, bank transfers, and VAs to collect and move value across borders. In this model, customers made low-value transfers through multiple channels, including wallets provided by foreign payment service providers in their home jurisdictions. Local and foreign operators then settled balances separately, using wire transfers, MVTS, VAs, or other value-transfer mechanisms. The typology also showed links to dealers in precious metals and stones, suggesting that high-value commodities may be used to settle balances or integrate value into the formal economy. Corporate vehicles and cover accounts were also used to channel funds through the banking system, often showing many-to-one transfers and cash activity inconsistent with the stated customer profile.

United Kingdom: UK authorities identified underground banking and HOSSP-based schemes combining bulk cash movement with commodity-based settlement. In this typology, criminal cash was introduced into the financial system through business bank accounts linked to shell or sham companies, often controlled by nominees. Large volumes of cash were also physically moved out of the UK,

including through passenger luggage, air freight, and shipments presented as legitimate wholesale cash transfers. One scheme involved couriers transporting over GBP 130 million (approximately USD 171 million) in cash to the UAE over a three-month period. The cash was declared on arrival as linked to a gold trading company and was allegedly used to purchase gold, including illicitly sourced material.

Box 33. Use of HOSSP networks for TF

Italy: Italian authorities identified a HOSSP-style value-transfer network used to move proceeds linked to migrant smuggling, with part of the funds channelled to terrorist organisations. The network relied on cash-based transfers through money or value-transfer channels and hawala-type arrangements. Financial flows were routed through third countries to Syria and involved actors connected to migrant smuggling, car dealerships, and transnational motor-vehicle trade. The same channels were used to move proceeds from organised crime and tax offences, creating overlapping criminal and TF risks. STRs helped identify concentrated flows through specific MVTS channels, links to high-risk jurisdictions, and shared actors across migrant smuggling, vehicle trade, and terrorist financing networks. Some individuals had direct links to Syria, including links to foreign terrorist fighters.

15. Establishing dedicated domestic co-ordination frameworks

Box 34. Dedicated domestic co-ordination frameworks against underground banking and HOSSP-based PML

China has implemented long-running special campaigns to address underground banking and HOSSP-based PML, including the nationwide Special Operation Against the Use of Offshore Companies and Underground Banking to Transfer Ill-Gotten Gains, jointly launched in 2015 by the People's Bank of China, the Ministry of Public Security, the Supreme People's Court, the Supreme People's Procuratorate and the State Administration of Foreign Exchange. The campaign is supported by joint analysis, information exchange and co-ordinated responses, and has been complemented by targeted crackdowns. China also uses standing co-ordination mechanisms, including the Interministerial Joint Conference on Anti-Money Laundering, established in 2002 and expanded to 22 authorities to support the sharing of underground banking leads and consultations on complex cases. The Action Plan for Combating and Addressing Money Laundering Crimes (2022–2024) further reinforced co-ordination, data sharing, and case feedback among supervisory, investigative, and judicial authorities.

Türkiye treats unlicensed MVTS, including HOSSPs, as illegal. The Central Bank of the Republic of Türkiye (CBRT) acts as the licensing authority and leads detection

and supervision of unlicensed operators. Criminal investigations are initiated through a written application by CBRT to the Public Prosecutor's Office. In parallel, FIU Türkiye (MASAK) develops financial intelligence on underground banking networks, typologies and predicate links, and transmits actionable intelligence to CBRT and prosecutors. CBRT has established a dedicated Payment Systems and Financial Technologies Department to handle unlicensed providers, including intelligence processing, technical assessments and complaints, while its legal department manages referrals and judicial follow-up. Indicators of unlicensed activity are received through government notifications, public and private complaints, and MASAK referrals. Cases follow a standardised workflow: CBRT technical assessment, audits or inspections where needed, referral of substantiated cases to prosecutors, and monitoring of proceedings. Permanent co-ordination is supported by Threat and Vulnerabilities Working Groups. The Threat Working Group co-ordinates responses to ML/TF threats, including underground banking, while the Vulnerabilities Working Group addresses systemic weaknesses, including in payment and e-money sectors, feeding into the NRA, policy, supervision and guidance.

16. Detecting underground banking and HOSSPs and developing actionable intelligence across public and private sectors

Box 35. Targeted PPPs to enhance detection and intelligence development against underground banking and HOSSP-related PML

Europol: Europol's Financial Intelligence Public Private Partnership (EFIPPP) strengthens detection and intelligence development on underground banking and HOSSP-related PML through structured engagement with public and private partners. EFIPPP gathers operational and strategic input through regular working groups, thematic work streams, plenary meetings, annual member questionnaires, and threat radar exercises. These mechanisms help identify emerging typologies, prioritise threats, and inform the development of shared guidelines, tools, and risk indicators. Operational co-operation is also supported through bilateral exchanges and case-specific information sharing in relevant investigations.

Box 36. Public outreach and reporting channels to detect illegal underground banking and HOSSP activity

Türkiye: In Türkiye, the Central Bank of the Republic of Türkiye operates a public notification mechanism for suspected unlicensed payment and remittance activity. Reports from individuals, institutions, and other authorities are assessed from a technical and legal perspective and, where substantiated, may be referred to prosecutors. Public communications and warnings on illegal MVTS activity support both deterrence and intelligence generation.

19. Deepening international co-operation

Box 37. Leveraging diverse international co-operation tools and networks to disrupt underground banking and HOSSP-based PML

Europol: Europol's activities on underground banking and HOSSP-based PML

Europol supports investigations into underground banking and HOSSP-based PML through operational task forces focused on high-value targets linked to parallel financial systems. These task forces bring together seconded investigators from concerned jurisdictions with Europol specialists and analysts. This enables faster information exchange, joint exploitation of operational data, including encrypted communications datasets, and use of Europol's analytical capabilities, asset recovery expertise, and VA tracing tools. Europol also supports broader co-operation through frameworks such as EMPACT, AMON, the Underground Banking Working Group, and the Europol Financial Intelligence Public-Private Partnership. These mechanisms help connect operational cases with strategic analysis, typology development, and cross-border co-ordination.

Nigeria: Cross-border co-operation to disrupt a gold-based underground banking arrangement

In 2025, Nigerian authorities, led by the Economic and Financial Crimes Commission in co-ordination with other stakeholders, investigated a fraud and ML case involving an underground banking arrangement. The case originated from the diversion of NGN 500,000,000 (approximately USD 346,000). Investigations identified a transnational scheme in which funds were settled outside the banking system through a gold-based mechanism. Nigerian funds were transferred to gold traders, who co-ordinated with counterparts in the United Kingdom to deliver equivalent cash to a nominee. The arrangement relied on intermediaries, corporate nominees, and, in part, VAs to obscure value flows. Given the cross-border structure—placement in Nigeria and cash-out abroad—authorities combined financial records, telecommunications data, and supervisory intelligence to reconstruct the transaction chain and identify overseas actors. This enabled timely engagement with foreign counterparts and supported potential mutual legal assistance. The case highlights the importance of early cross-border co-operation in schemes involving offshore settlement. By combining informal information exchange with formal co-operation tools, authorities were able to identify beneficiaries, trace assets, and support co-ordinated disruption of the underground banking network.

Switzerland: International roundtable on underground banking

In November 2025, Switzerland hosted the second international roundtable on underground banking in Bern, convened by the Money Laundering Reporting Office Switzerland within fedpol. The event brought together law enforcement, FIUs, and international organisations, including INTERPOL, Europol, and UNODC, to exchange insights on underground banking mechanisms, investigative practices, and disruption strategies. Discussions focused on the misuse of informal payment systems for ML, TF, and sanctions evasion, and highlighted the importance of typology development, timely information exchange, and co-ordinated cross-

border action. This multi-stakeholder dialogue illustrates a good practice for strengthening detection, intelligence sharing, and co-ordinated responses to underground banking and HOSSP-based PML schemes.

September 2026

www.fatf-gafi.org