Guide on Following the Money in Trafficking in Persons Cases

A practical guide for investigating financial crime related to trafficking in persons cases

The Bali **Process**

The Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime (the Bali Process) was established in 2002 and is a voluntary and non-binding regional consultative process co-chaired by the Governments of Australia and Indonesia and comprising over 45 member countries and organisations.

The Regional Support Office of the Bali Process (RSO) extends its gratitude to the Australian Government Department of Home Affairs, which has provided primary funding for the RSO since its establishment in 2012, and to the International Organization for Migration (IOM), which hosts the RSO in Bangkok, Thailand and supports its administration. The RSO thanks the Royal Thai Government for its ongoing support for the RSO to operate in Bangkok, Thailand.

The work of the RSO would not be possible without the support and commitment of Bali Process members, each of whom contribute time, resources, and personnel to work with the RSO.

Queries about this guide should be addressed to the Regional Support Office (RSO) to the Bali Process at:

Regional Support Office of the Bali Process (RSO)
27th Floor Rajanakarn Building, 3 South Sathorn Road, Sathorn, Bangkok 10120, Thailand,
Tel: +66 2 343 9477 Fax. +66 2 676 7337
Email: info@rso.baliprocess.net, www.rso.baliprocess.net

Drafting Committee to Update the *Bali Process Guide on Following the Money in Trafficking in Persons Cases*

Ian Warne
Second Secretary,
Department of Home Affairs, Australia

Josie Chantrell
Assistant Director,
Attorney-General's Department, Australia

Al Mamun
Criminal Investigation Department,
Bangladesh Police

Md. Jaynul Abedeen
Joint Director,
Bangladesh Financial Intelligence Unit

Rachna Chhokar
Deputy Director,
Directorate of Enforcement, India

Deandra Cinuti Raryarasmi
Attaché, Directorate of International Peace and Security, Directorate General of Multilateral Affairs, Ministry of Foreign Affairs of Indonesia

Roy Suganda Putra Sinurat
Police Senior Inspector,
Trafficking in Person Task Force,
Sub Directorate V, Directorate of General Crime,
Indonesian National Police

Sonora Gokma Pardede
Prosecutor,
Attorney-General's Office of the Republic of Indonesia (Kejagung)

Tri Andriyanto
Senior Financial Transaction Analyst,
Indonesian Financial Transaction Reports and Analysis Center (PPATK), Directorate of Strategy and International Cooperation

---

Irfan Azim Burni
Acting Deputy Director,
Federal Investigation Agency of Pakistan

Ian Wong
Deputy Director,
Ministry of Home Affairs, Singapore

Rayna Tan
Senior Manager,
Ministry of Home Affairs, Singapore

Thapana Bhasathiti Sanyabutra
Special Case Officer, Professional Level,
Department of Special Investigation, Thailand

Saengduen Sangbuarngamlom
Acting Director of Financial Investigation Sub-Division/Investigator, Professional Level,
Anti-Money Laundering Office, Thailand

Prapawin Manyawuth
Deputy Director of Bureau of Human Trafficking Crime, Department of Special Investigation, Bureau of Human Trafficking Crime,
Ministry of Justice, Thailand

Aron Marcellus
Assistant Attache,
Homeland Security Investigations, U.S. Embassy, USA

Observers to the Drafting Committee to Update the *Bali Process Guide on Following the Money in Trafficking in Persons Cases*

Melissa Sevil
Director - TA & Typologies, Asia/Pacific Group on Money Laundering

Stephen Munro
Deputy Director, TA & Typologies, Asia/Pacific Group on Money Laundering

Chengyi Ong
Head of Policy, APAC, Chainalysis, Inc

Jill Huinder
Project Coordinator Finance and Human Rights, Finance Against Slavery and Trafficking Initiative (FAST), UNDP

The RSO would like to thank Kristina Amerhauser for supporting the initial development of this guide, and to acknowledge the Global Initiative Against Transnational Organized Crime (GI-TOC) and ASEAN-Australia Counter Trafficking (ASEAN-ACT) for co-facilitating the workshop that led to the establishment of the Drafting Committee.

FOREWORD

Since its inception in 2002, the Bali Process on People Smuggling, Trafficking in Persons, and Related Transnational Crime has supported Member States in their efforts to address the impacts of people smuggling, trafficking in persons, and related transnational crime through developing and implementing strategies and practical forms of cooperation to address these challenges. Co-chaired by the Governments of Indonesia and Australia, the Bali Process brings together more than 48 members, including 45 Member States and the United Nations High Commissioner for Refugees (UNHCR), the International Organization for Migration (IOM), the International Labour Organization (ILO) and the United Nations Office on Drugs and Crime (UNODC), alongside Observer States and organisations.

At the sixth Bali Process Regional Ministerial Conference in March 2016, ministers underscored the importance of States' obligations to criminalise money laundering and the proceeds of crime as a means of reducing the financial incentives that underpin people smuggling and trafficking in persons. Ministers recommended that the Bali Process Working Group on Trafficking in Persons (the Working Group) deliver targeted training and develop regional guidance on this issue. In May 2016, the Working Group convened the Bali Process Following the Money Forum, which in turn recommended the development of a regional policy guide and an associated training module focused on the use of financial investigation tools in trafficking in persons cases.

Following these recommendations, the Working Group established a drafting committee, co-chaired by the Governments of Indonesia and Australia, to prepare the first policy guide on following the money in trafficking in persons cases. This guide was finalised and endorsed in October 2017 and subsequently published in 2018.

In the years since the original guide was released, the trafficking in persons landscape has evolved significantly. Member States, notably during the Regional Support Office of the Bali Process' (RSO's) 2nd and 3rd Constructive Dialogues, expressed a need for clearer guidance on the role of virtual assets such as cryptocurrencies and for additional context within the guide related to emerging trafficking trends, such as trafficking for forced criminality into cyber-scam centres. This updated version of the guide reflects these developments and has also been revised to enhance usability, with the objective of more directly serving as a bridge between counter-trafficking law enforcement and financial investigators. By supporting a clearer understanding of respective roles and methodologies, the guide aims to facilitate stronger coordination as investigations progress at the intersection of illicit finance and trafficking in persons.

These updates align with the outcomes of the 2023 Bali Process Ministerial Conference and the priorities set out in the Adelaide Strategy for Cooperation. The Adelaide Strategy emphasises comprehensive approaches to detecting, preventing, investigating, and prosecuting people smuggling, trafficking in persons, and related transnational crime, including cyber-scam centre operations. It further highlights the importance of strengthening law enforcement capacity to address technology-facilitated trafficking and people smuggling, as well as enhancing collaboration between regional law enforcement agencies and relevant regional organisations. Engagement between Bali Process Members and Drafting Committee Members/Observers has been central to advancing these priorities and has directly informed the development of this guide.

This updated guide builds on the foundations of the original and was developed through a collaborative drafting process coordinated by the RSO. A Drafting Committee comprising experts on anti-money laundering and trafficking in persons from Australia, Bangladesh, India, the Republic of Indonesia, Pakistan, Singapore, Thailand, and the United States of America met on four occasions over the past 18 months to review and refine successive drafts, alongside Observers from the Asia/Pacific Group on Money Laundering (APG), Chainalysis, and the United Nations Development Programme's Finance Against Slavery and Trafficking (FAST) Initiative. The RSO thanks all Drafting Committee Members and Observers for the significant time and expertise contributed to this process and is confident that these collective efforts have resulted in a guide that is practical and usable for practitioners.

Developed through extensive consultation and informed by the operational experience of practitioners across the region, this guide reflects the Bali Process' continued commitment to practical cooperation and to strengthening collective responses to trafficking in persons and related transnational organised crime. By addressing the financial dimensions of these crimes and the growing convergence between trafficking, fraud, and technology-facilitated exploitation, the guide aims to support more effective coordination between counter-trafficking and financial investigation efforts. It is hoped that this guide will serve as a useful and enduring reference for practitioners across the Bali Process region, helping to bridge knowledge and practice between counter-trafficking and financial crime criminal justice actors.

LIST OF FIGURES

ABBREVIATIONS

ACTIP	ASEAN Convention against Trafficking in Persons
AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
ARINs	Asset Recovery Inter-Agency Networks
ARRP	Anti-Money Laundering Rapid Response Protocol
BPMS	Bali Process Member State
BTC	Bitcoin
CBC	Conviction based confiscation
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CSO	Civil society organisation
CTR	Currency transaction reports
DeFi	Decentralised finance
DNFBP	Designated non-financial businesses and professions
ED	Enforcement Directorate
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FIUs	Financial intelligence units
IGRIA	INTERPOL Global Register of Illicit Assets
IGRIP	INTERPOL Global Rapid Intervention of Payment
ILO	International Labour Organization
KYC	Know-your-customer
LEAs	Law enforcement agencies
ML	Money laundering
MLA	Mutual legal assistance
MO	Modus operandi

MVTS	Money or value transfer services
NCBC	Non-conviction based confiscation
NRA	National Risk Assessment
OCSE	Online child sexual exploitation
OJK	Otoritas Jasa Keuangan / Financial Service Authority
OSCE	Organization for Security and Co-operation in Europe
OTC	Over-the-counter
P2P	Peer-to-peer
PF	Proliferation financing
RBA	Risk-based approach
SEZs	Special economic zones
SRA	Sectoral Risk Assessment
STR	Suspicious transaction reports
TBML	Trade-Based Money Laundering
TI	Telecommunications interception
TIP	Trafficking in persons
TOC	Transnational organised crime
TTR	Threshold transaction reports
UNCAC	United Nations Convention Against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention Against Transnational Organized Crime
VAs	Virtual assets
VASP	Virtual asset service providers

TABLE OF CONTENTS

INTRODUCTION

Trafficking in persons (TIP) continues to be a harmful and pervasive crime across the Asia Pacific region. It exploits women, men and children, and diverts billions of US dollars in illicit proceeds from the legitimate economy into the operations of transnational organised crime (TOC).

These challenges are occurring in parallel with broader transformations in the global financial and technological landscape. The increasing use of virtual assets, the accelerated adoption of digital identification systems, and the ongoing digitisation of financial services have opened new pathways for financial flows. Further, transnational organised crime groups have adapted rapidly to these changes, harnessing financial technology (fintech) applications and virtual assets (such as cryptocurrencies) in moving and laundering proceeds stemming from TIP.

Though not as swiftly, government responses have also evolved—through regulatory reform, improved international coordination and enhanced enforcement capabilities. These dynamics reinforce the importance of updating this guide to reflect current realities and equip stakeholders with the tools required to meet a rapidly evolving threat environment.

To support Member States in this evolving landscape, the Bali Process has published this update to the original *Policy Guide on Following the Money in Trafficking in Persons Cases* from 2018. This guide supports Member States to target the illicit proceeds of transnational organised crime and all those trafficking in persons.

The updated guide addresses the evolutions in TIP and illicit financial flows to reflect current and emerging threats, challenges and best practices. Core themes in this update include:

- Methods to generate, move and conceal illicit proceeds across borders, including virtual assets (e.g. financial technology, cryptocurrencies), cash payments/smuggling and hawala and informal value transfer systems.
- The diversity and complexity of TIP (e.g. forced labour, sexual exploitation, online child sexual exploitation), leading to distinct patterns of financial crime requiring bespoke and purposeful responses from law enforcement in 'follow-the-money' approaches.
- Increased interconnectedness (e.g. uptake of digitalisation) requiring increased coordination of domestic, regional and international agencies to effectively identify, trace, investigate and ultimately confiscate illicit proceeds.

- Increased role of multilateral organisations, the private sector and civil society in supporting domestic, regional and international cooperation efforts, providing accurate data and analysis, and supporting training and capacity-building.

By focusing on these core themes, and with an emphasis on the profit-driven nature of trafficking in persons, this guide aims to support those working to counter both TIP and financial crime. It provides strategic guidance and practical tools to help disrupt the financial flows that sustain trafficking in persons operations, and to strengthen coordinated responses to effectively combat TIP.

SECTION 1

RATIONALE

Like most transnational crimes, trafficking in persons is fundamentally profit-driven, generating billions in illicit proceeds while causing significant harm to individuals and communities. Criminal networks exploit vulnerable populations through various forms of trafficking, further moving and laundering their illicit proceeds in an increasingly diverse and creative range of typologies.

The scale of this challenge is immense, with data indicating that financial crimes are now the most prevalent criminal market, with cyber-dependent crimes also expanding rapidly, alongside trafficking in persons.[1] The Asia Pacific region is particularly impacted, serving simultaneously as a place of origin, transit and destination for victims of trafficking. The Asia Pacific region has experienced a wide range of forms of trafficking, such as forced labour, child labour, sexual exploitation, debt bondage and involuntary servitude among migrant labourers. The region has also seen the emergence of cyber-enabled crime types, such as online child sexual exploitation (OCSE) and trafficking for forced criminality into cyber-scam centres.

The economic impact of TIP is difficult to measure, however, the International Labour Organization (ILO) estimates that the profits from forced labour amount to USD $236 billion per year.[2] In addition, scams were one of the biggest drivers of cryptocurrency-based crime, accruing at least USD $9.9 billion in 2024.[3] However, these estimates of illicit proceeds likely represent only a fraction of the total scale.

The diversity of forms of TIP requires sophisticated responses adapted to both the specific crime type and local/regional contexts. Each trafficking typology involves differing modus operandi for the generation and laundering of the proceeds of crime, thus requiring inter-agency cooperation and cross-thematic knowledge sharing between TIP investigators and financial investigators to support successful investigations. Financial investigators should understand these distinctions in order to appreciate differences in trafficking typologies and how these lead to differing indicators or patterns of suspicious transactions, differences between financial investigations and trafficking investigations, and the types of material evidence that can be obtained and used for investigations and prosecutions. Understanding financial crime flows and typologies—from initial exploitation to money laundering (ML)—is critical for disrupting TIP and transnational crime, as well as for providing justice for victims.

1 Global Initiative against Transnational Organized Crime (2025) *Global Organized Crime Index 2025: Crime at a Crossroads*. Available at: https://globalinitiative.net/wp-content/uploads/2025/11/Global-Organized-Crime-Index-2025-Crime-at-a-Crossroads-GI-TOC-November-2025.pdf

2 International Labour Organization (2024) *Profits and Poverty: The Economics of Forced Labour* (second edition). Available at: https://www.ilo.org/media/520201/download

3 Chainalysis (2025) *The 2025 Crypto Crime Report: The Rising Role of Cryptocurrency in All Forms of Crime and How Its Transparency Is Creating Unique Opportunities for Investigation*. Available at: https://static1.squarespace.com/static/66e849ec2d805d56b4474766/t/67d96cfdbcb5f62c46476863/1742302487949/the-2025-crypto-crime-report-release-compressed.pdf

Given that TIP is fundamentally profit-oriented, strategies that 'take the profit out of crime' have seen success at identifying, investigating and disrupting transnational crime. Over the past decade, 'following the money' has become a core part of the response to a range of transnational crimes including TIP, complementing other law enforcement responses.

The Relationship Between Financial and Trafficking Investigations

Financial investigations and TIP investigations serve distinct but complementary purposes. While TIP investigations typically focus on identifying and prosecuting perpetrators, and protecting victims, financial investigations centre on identifying, tracing, seizing and confiscating proceeds of crime.

Financial investigations may be initiated in parallel with TIP investigations or independently, for example, where suspicious financial activity is identified before the underlying criminal conduct is known. It is strongly recommended that financial investigations run concurrently with TIP investigations to maximise impact, improve evidentiary outcomes, and identify broader criminal networks, assets and facilitators.

Effective coordination between law enforcement, financial intelligence units (FIUs), prosecutors and other stakeholders is essential to ensure that both types of investigations reinforce each other, with financial investigations providing insight into the structure and operation of transnational organised crime groups and potential leads on recruitment, movement, or exploitation of victims.

As this guide details, the key objective of a financial investigation is to identify and trace the proceeds and instruments of crime linked to suspected criminal activity, with the ultimate goal of depriving criminals of their profits and assets. As criminal enterprises engage in criminality for profit and further rely on money to fund their illicit activities, these investigations can generate valuable information regarding criminal activities, methodologies and actors involved.[4] Financial crime, such as ML, is dependent on the commission of a predicate crime, such as TIP.

The Financial Action Task Force (FATF)[5] sets global minimum standards for anti-money laundering (AML) to prevent and combat financial crime, including in relation to conducting ML investigations and asset recovery.[6] All jurisdictions are assessed regularly for compliance with the FATF Standards, taking into account their unique risks

4 Regional Support Office of the Bali Process (2018) *Policy Guide on Following the Money in Trafficking in Persons Cases*. Available at: https://s3.ap-southeast-2.amazonaws.com/assets.baliprocess.net/app/uploads/2022/01/19142902/Bali-Process-Guide-WEB-v01-1-9english3.pdf

5 The Financial Action Task Force is a 40-member intergovernmental body with responsibility for setting international standards on anti-money laundering, countering the financing of terrorism and counter-proliferation financing.

6 Financial Action Task Force (2012, updated June 2025) *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*. Available at: https://www.fatf-gafi.org/en/topics/fatf-recommendations.html

and context, and whether they are effectively implementing proportionate measures to address their identified risks.[7] Some factors that often impact Asia Pacific risk profiles include unregulated informal cash-based economies, special economic zones (SEZs), and gaps in regulatory measures.[8]

1.1 Purpose of this guide

The guide aims to identify opportunities for increased collaboration between the counter-trafficking and financial crime communities, across both the private and public sector, e.g. policymakers, FIUs and law enforcement agencies (LEAs). As officials working in these sectors frequently deploy specialised expertise, these areas are often siloed from one another. Counter-trafficking in persons agencies may be unaware of, or not trained to handle, financial activity related to trafficking in persons. Conversely, financial investigators may lack detailed knowledge of TIP-related laws, trends and methodologies. Bringing these perspectives together wields significant potential to amplify the effectiveness of the overall response.

This guide offers insights into how illicit proceeds from trafficking in persons are generated, held, moved and integrated, with the aim of supporting practitioners working across the trafficking and financial crime sectors to identify key actors, understand their methodologies and strengthen collaboration. It provides an overview of the different TIP crime types as well as the distinct methods used to generate, move and launder illicit proceeds from those crimes. Where available, the guide also offers case studies, flags key challenges and provides practical suggestions for improving investigative outcomes.

While this guide focuses on the financial dimensions of trafficking in persons, it is important to recognise that the impacts of trafficking are far broader. Trafficking in persons is first and foremost a violation of human rights, with victims frequently enduring serious long-term psychological distress and physical abuse. The crime also generates significant social and economic harm in affected communities and is often enabled by corruption that weakens the rule of law, undermines good governance and erodes trust in local institutions. A holistic response to trafficking in persons should therefore account for its human, financial, societal and environmental consequences.

Efforts to counter TIP have traditionally focused on pursuing the trafficking offence, and not on the proceeds derived from or invested in the crime.[9] Incorporating a 'follow-the-money' approach strengthens this response by generating financial intelligence that can support successful prosecutions, uncover additional leads and co-conspirators, and more systematically disrupt the networks that sustain trafficking operations. Financial investigation can also hinder the ability of organised crime groups to reinvest proceeds into further criminal activity, while providing agencies with a mechanism to channel recovered assets into community or victim-focused initiatives.

[7] Asia/Pacific Group on Money Laundering. *FATF Standards.* Available at: https://www.apgml.org/about-us/fatf-standards

[8] International Centre for Criminal Law Reform and Criminal Justice Policy. *Money Laundering in the Asia Pacific.* Available at: *https://icclr.org/wp-content/uploads/2019/06/Paper1.pdf?x92730*

[9] Organization for Security and Co-operation in Europe (2014) *Leveraging Anti-Money Laundering Regimes to Combat Trafficking in Human Beings.* Available at: https://www.osce.org/secretariat/121125?download=true

1.2 Scope of this guide

This guide focuses on TIP investigations and the intersection with the laundering of illicit funds associated with these cases. While TIP comes in a number of forms—some of which overlap—this guide will focus on the following types of trafficking:

- forced labour
- online child sexual exploitation
- commercial sexual exploitation
- forced criminality

These forms of TIP are often associated with specific, readily identifiable financial behaviours and profiles, which can in turn assist investigators and FIUs and lend themselves best to a blended investigation. They are also considered likely to lead to the confiscation of criminal assets and subsequent successful criminal prosecutions. Importantly, asset confiscation can, and where permitted should, occur prior to prosecution, whether through non-conviction-based confiscation in jurisdictions that allow it or through provisional measures such as freezing and seizing orders. Acting early in this way reduces the risk of asset flight, as the initiation of a criminal investigation can prompt traffickers to rapidly move, conceal or dissipate their assets before any confiscation order can take effect. These approaches are examined in further detail in Sections 2 and 3.

Trafficking in relation to forced labour

Trafficking in persons for the purpose of forced labour involves the recruitment, transportation, transfer, harbouring, or receipt of persons by traffickers, including transnational organised crime groups, through means such as coercion, deception, abuse of power or of a position of vulnerability, or debt bondage, for the purpose of exploitation.

Forced labour encompasses any work or service extracted from a person under the menace of penalty and without their free and voluntary consent, including the freedom to leave at any time.[10]

[10] International Labour Organization. *What is forced labour?* Available at: https://www.ilo.org/topics/forced-labour-modern-slavery-and-trafficking-persons/what-forced-labour

Trafficking for online child sexual exploitation

The recruitment, transfer, harbouring or receipt of a child through deception, coercion, or abuse of a position of vulnerability, where digital tools and online platforms are used to facilitate any stage of that process, for the purpose of sexual exploitation. The exploitation itself may take a range of forms, including the production, distribution, or possession of child sexual abuse material (CSAM); the live-streaming of child sexual abuse; the grooming of a child for sexual purposes; or the sexual extortion of a child. In some instances, the abuse is committed or directed entirely remotely, without any physical movement of the child.[11]

Trafficking for forced commercial sexual exploitation

Forced commercial sexual exploitation involves compelling a person, through force, coercion, abduction, fraud, deception, abuse of power or of a position of vulnerability, or debt bondage, to engage in commercial sex acts for the financial benefit of another.

Exploitation can include forced prostitution, sexual servitude, or the use of victims in the production of sexual abuse material. The consent of a victim is irrelevant where any of the above means have been used.[12]

Trafficking for the purpose of forced criminality

Trafficking for the purpose of forced criminality is a form of trafficking in persons in which victims are exploited through being compelled to commit criminal acts for the economic or other gain of traffickers or exploiters.[13]

Across all forms of trafficking in persons, where the victim is a child, the means element does not need to be established: the recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation constitutes trafficking in persons regardless of whether coercion, deception or any other means were employed.

[11] Interagency Working Group on Sexual Exploitation of Children (ECPAT International, lead organisation) *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, Second Edition. Bangkok: ECPAT International, March 2025.
[12] Walk Free. *Global Slavery Index: Terminology.* Available at: https://www.walkfree.org/global-slavery index/methodology/terminology/
[13] United Nations Office on Drugs and Crime (UNODC) Regional Office for Southeast Asia and the Pacific. *Explainer: What is trafficking for forced criminality?* Available at: https://www.unodc.org/roseap/en/2024/10/ trafficking-forced-criminality/story.html

SECTION 2

UNDERSTANDING MONEY LAUNDERING AND ASSOCIATED RISKS, THREATS AND VULNERABILITIES IN TRAFFICKING IN PERSONS

2.1 Understanding the risks, vulnerabilities and typologies of financial crime associated with trafficking in persons

Risk occurs when a **threat** (e.g. criminal network) successfully takes advantage of a **vulnerability** (e.g. unregulated sector) to produce a consequence (e.g. facilitator of TIP).[14] In the ML risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the inherent features of a particular sector, financial product or type of service that make them attractive for ML purposes.

While the specific sectors, typologies and factors that are vulnerable to ML or TIP vary greatly between jurisdictions, and should be identified and assessed regularly by every jurisdiction, this guide aims to highlight vulnerabilities known to be prevalent in the Bali Process region.

Risk and context

The ML and TIP risks, threats and vulnerabilities vary significantly between jurisdictions, and are further informed by the specific **risk and context** of each country, region or city.

Some factors that may indicate an increased TIP or ML (arising from TIP) risk include:

- high volume of cash transactions
- low per capita income levels or limited employment opportunities
- weakened government controls or political commitment
- geographic factors, particularly in areas with porous borders

[14] Financial Action Task Force (2024, updated 2025) *Money Laundering National Risk Assessment Guidance.* Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Guidance.html

Indonesia’s Risk Assessment and Supervision Framework: OJK and FATF Alignment

In line with Recommendation 1 of the FATF Standards, the Republic of Indonesia, through its Financial Service Authority (Otoritas Jasa Keuangan/OJK), fulfils the Recommendation to identify, analyse, and evaluate ML risks through national legislation harmonisation related to AML, counter-terrorist financing (CFT) and proliferation financing (PF), particularly the issuance of OJK Regulation No. 12 of 2017, as well as the development of supporting systems and awareness-raising initiatives for the Financial Services Sector. The Republic of Indonesia develops a comprehensive Sectoral Risk Assessment (SRA) for the Financial Services Sector to ensure systematic risk mitigation and to establish clear priority areas based on identified threats and vulnerabilities. The Republic of Indonesia also strengthens supervision of the implementation of AML/CFT and PF programmes through a robust risk-based approach (RBA), ensuring that supervisory focus and resources are proportionately directed to higher-risk areas.

The prevalence of certain ML methods (or ‘typologies’) varies between crime types, perpetrators and jurisdictions due to the unique context that criminals operate in.

In implementing AML measures to combat TIP, jurisdictions should adopt a risk-based approach (RBA). In the context of TIP, an RBA allows jurisdictions to direct limited resources toward the money laundering typologies and channels most commonly associated with trafficking in their specific context. There are a range of risk assessment tools to support Member States, including the FATF ML National Risk Assessment (NRA) Guidance and Sectoral Risk Assessments (SRAs), which can be particularly valuable for sectors commonly exploited in TIP-related money laundering such as money or value transfer services, real estate and cash-intensive businesses.[15]

2.2 How is money laundered?

TIP generates significant illicit proceeds which, as with all transnational crimes, serve as the primary motivator for this criminal activity. In order to benefit from these illicit proceeds and avoid detection from competent authorities, criminal groups need to ‘launder’ the proceeds of their crimes. FATF describes ML as the process of making the proceeds of crime appear legitimate, typically through converting, transferring or concealing illicit property to hide its criminal origin and prevent legal consequences.[16]

[15] Financial Action Task Force (2024, updated 2025) *Money Laundering National Risk Assessment Guidance.* Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Guidance.html

[16] Asia/Pacific Group on Money Laundering (APG). *FATF Standards.* Available at: https://www.apgml.org/about-us/fatf-standards

While the ML process can include various steps, it is usually separated into three broad stages: placement, layering and integration, as set out below.[17]

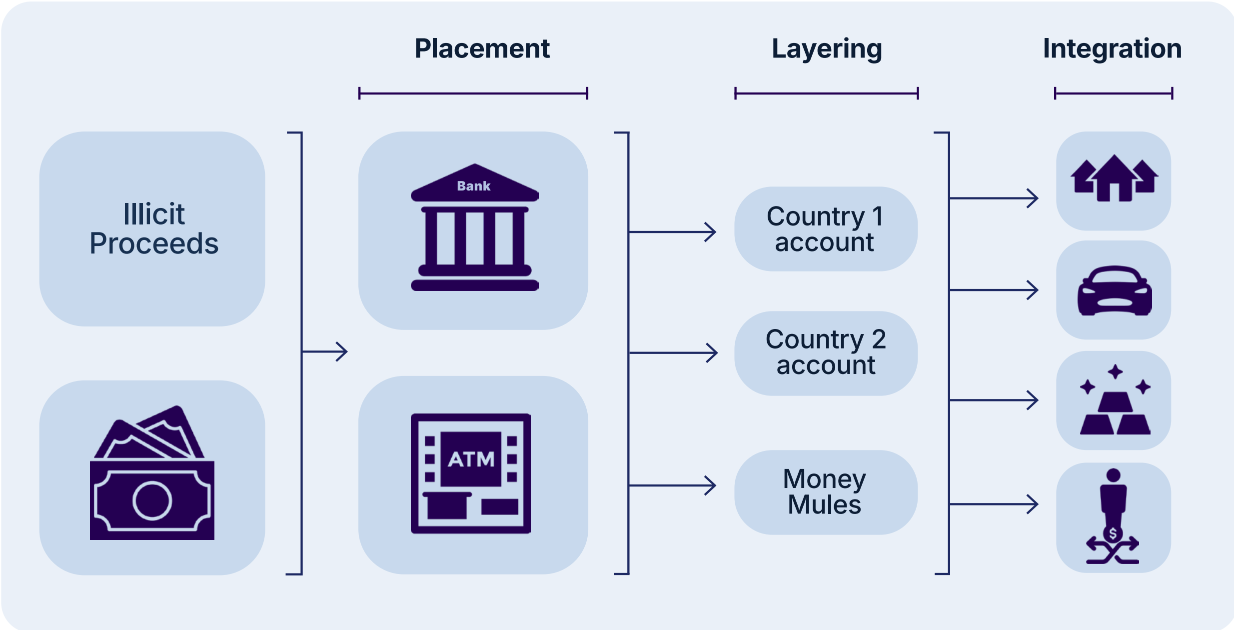
Placement: Placement involves bringing the illegal funds or assets into the financial system. Methods employed may include depositing cash into bank accounts or purchasing assets with cash. For instance, criminals might use illicit cash to acquire high-value items, which can later be sold to 'legitimise' the proceeds of crime.

Layering: Layering involves concealing the illegal origin of the placed funds by moving or disguising them. At this stage, the objective is to obscure the illicit origin of the funds through a series of complex transactions. Techniques may involve transferring funds across multiple accounts, often spanning various institutions and jurisdictions, or converting the funds into different financial instruments. The use of professionals, such as lawyers or accountants, to act as intermediaries, or the creation of complex company and trust structures, are common methods to further disguise the money's origin.

Integration: Integration occurs once the funds are layered and distanced from their origins and can be made available for criminals to use and control as ostensibly legitimate funds through being reintroduced into the legitimate economy, making them available for use by criminals as seemingly clean money. This can manifest through investments in legitimate businesses, such as purchasing shares in companies or acquiring high-value assets such as real estate and luxury goods.

[17] United Nations Office on Drugs and Crime, *Overview: Money Laundering*. Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html

Figure 1: Overview of the money laundering process.



2.3 Money laundering risks related to trafficking in persons

Each trafficking typology involves distinct methods of generating and laundering the proceeds of crime, requiring close inter-agency cooperation between trafficking investigators and financial investigators. To facilitate effective coordination, financial investigators should understand:

To facilitate effective coordination, financial investigators should understand:

- The distinctions between trafficking typologies and how these differences manifest in varying financial indicators or patterns of suspicious transactions.
- Differences between financial investigations and trafficking investigations.
- Material evidence that can be obtained and used for investigations and prosecutions related to both TIP and related financial crimes.

The diversity of the Bali Process region is reflected in both the variety of forms in which TIP occurs and the range of contexts in which these crimes take place. Trafficking networks target different demographics in various locations for different types of exploitation and use diverse payment and transfer mechanisms to conceal illicit proceeds. Diverse factors guide the choice of payment and money laundering mechanisms, including:

- The type of TIP.
- The size and scale of illicit proceeds that require laundering.
- The size of the transnational criminal organisation, its capacity and technological expertise, and the transfer mechanisms available to it.
- The risk and context—this includes the characteristics and size of the local economy and the structure of its financial system, i.e. the type of accessible financial institutions and the availability of fintech and cryptocurrencies.

A significant challenge in harnessing financial investigations for effective counter-trafficking efforts remains a lack of comprehensive data and risk understanding across countries. For example, a 2018 FATF report on TIP-related financial flows examined 28 National Risk Assessments (NRA) from a range of jurisdictions. Only 14 of those identified TIP as a ML risk and only four classified such risks as high.[18] The FATF requires all jurisdictions to identify and assess their money laundering risks. However, relatively few countries have specifically identified TIP-related money laundering within their national risk assessments, and fewer still have assessed it as high-risk. This picture is difficult to reconcile with data indicating billions in profits generated from trafficking in persons annually.[19][20]

Such figures suggest that the financial dimensions of TIP may be under-recognised or insufficiently analysed in risk assessments, indicating a gap in awareness of the linkages between TIP and financial crime that can lead to a lack of prioritisation in legal/regulatory frameworks or throughout law enforcement investigations.

In line with the FATF Standards—global recommendations to combat ML through financial system integrity, transparency and effective law enforcement—jurisdictions should effectively identify and assess their ML risks, including, where relevant, those arising from TIP. Given that civil society organisations often hold frontline knowledge of trafficking patterns and the private sector sees related financial indicators firsthand, their participation in the development of risk assessments can significantly strengthen the quality and accuracy of this analysis. [further discussion in Section 4].

18 Financial Action Task Force and Asia/Pacific Group on Money Laundering (2018) *Financial Flows from Human Trafficking*. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Human-Trafficking-2018.pdf

19 International Labour Organization (2024) *Profits and Poverty: The Economics of Forced Labour*. Available at: https://www.ilo.org/sites/default/files/2024-10/Profits%20and%20poverty%20-%20The%20economics%20of%20forced%20labour_WEB_20241017.pdf

20 Global Initiative Against Transnational Organized Crime (2025) *Compound crime: Cyber scam operations in Southeast Asia*. Available at: https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf

CASE STUDY - Financial Crime Arising From Cross-Border Trafficking For Sexual Exploitation

Indian police initiated a criminal case following the trafficking of a girl from Country B, who was smuggled into India using fraudulent identity documents. After being taken to Ranchi, Jharkhand, under false pretences and promised employment in a beauty parlour, the victim was instead forced into prostitution. She later escaped and provided information that enabled police to conduct raids at multiple locations.

The trafficking investigation identified indicators that the exploitation was organised and profit-driven, including the involvement of recruiters, transport facilitators and intermediaries, and regular payments linked to the exploitation of multiple victims. These findings were referred to India's Enforcement Directorate (ED)[21], enabling the initiation of a parallel financial investigation.

By analysing financial and communications data alongside information from the trafficking case, the ED established that the criminal activity extended beyond an isolated trafficking offence and formed part of a broader organised network. This included illegal border crossings, the use of fraudulent identity documents, and facilitation of unlawful residence in India.

The combined trafficking and financial investigations enabled searches at 17 premises across several Indian states, resulting in the seizure of fake identity documents, weapons, jewellery, a forged passport, and other incriminating materials. Four individuals were arrested.

The financial investigation identified a network of brokers operating in Country B who facilitated recruitment and transportation of women and received commissions of approximately USD $150–200 per victim. Organisers of the network received fixed monthly payments of approximately USD $1,000–1,200 per victim from those exploiting the women.

Financial analysis demonstrated that the syndicate's leaders had accumulated significant assets, including real estate and jewellery, grossly disproportionate to their declared incomes. The illicit proceeds, heavily reliant on street-level cash collections and digital micro-transactions, were laundered through a complex web of sham entities—including a fake charitable foundation, hospitality fronts, and construction enterprises. These assets were frozen and seized, and a comprehensive prosecution complaint was filed before a specialised anti-money-laundering court.

[21] The Enforcement Directorate is a multi-disciplinary organisation mandated with the investigation of money laundering offences and violations of foreign exchange laws.

Virtual assets including cryptocurrency

Rapid evolutions in technology, such as artificial intelligence (AI), digital identities and virtual assets (VAs), have led to drastic changes in the transnational crime landscape. The growing accessibility of tools to carry out criminal activity, such as deepfake software, large language models, generative AI and stolen personal data, has dramatically increased the capability of criminal actors to engage in new and sophisticated forms of fraud and crime. In recent years, the number of cyber-scam centres has exploded in the region, with trafficking in persons to support this threat commensurately increasing. Increased virtual asset adoption across both licit and illicit domains has created new opportunities for criminals to generate and launder illicit proceeds, presenting challenges for law enforcement in tracing assets internationally.

VAs, encompassing non-fiat digital representations of value, such as cryptocurrencies,[22] have become integral to the global financial landscape. While they offer innovative solutions to issues such as financial inclusion,[23] their characteristics—such as anonymity, decentralisation, and rapid transaction capabilities—make them susceptible to misuse by criminal entities, including those involved in TIP. The Financial Crimes Enforcement Network (FinCEN) reported a significant increase in Bank Secrecy Act filings related to TIP and the use of convertible VAs,[24] indicating a growing trend in the utilisation of VAs within trafficking operations.

The swift advancement of VAs and their supporting technologies often outpaces the development of regulatory frameworks, creating vulnerabilities and gaps that traffickers can exploit. Jurisdictional discrepancies can complicate international cooperation efforts, while the capacity of jurisdictions to identify and investigate such activity can further hinder effective counter-trafficking efforts.

Cyber-scam operations and compounds

Cyber-scam operations in Southeast Asia are highly sophisticated, industrial scale, and specialise in social engineering techniques. Cyber-scams are often carried out by people who are forced to participate and are exploited for the purpose of forced criminality; hundreds of thousands of nationals from more than 70 countries have been reported to have been deceived and trafficked into cyber-scam compounds in Myanmar, Cambodia and Laos. These operations exemplify a convergence of various forms of transnational organised crime, including trafficking in persons, cyber-enabled crime, corruption, money laundering and fraud.

[22] That is, they do not include digital representations of 'fiat currency', i.e. money in a bank account.

[23] Financial Action Task Force (2019) *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers.* Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf.coredownload.inline.pdf

[24] Financial Crimes Enforcement Network (2024) *FinCEN Sees Increase in BSA Reporting Involving the Use of Convertible Virtual Currency for Online Child Sexual Exploitation and Human Trafficking.* Available at: https://www.fincen.gov/news/news-releases/fincen-sees-increase-bsa-reporting-involving-use-convertible-virtual-currency

Large parts of cyber-scam operations in Southeast Asia and beyond are based in cyber-scam compounds, which are buildings that have been constructed or repurposed to host criminal groups seeking premises for illegal online businesses. The compounds generally provide security, internet, management, financial services and some measure of protection from law enforcement campaigns. The compounds themselves, or often the transnational organised crime groups operating these compounds, impose controls on freedom of movement. From remote regions to urban areas, these centres are based in plain sight, including at hotels, resorts, apartments, casinos and purpose-built compounds.

Cyber-scam operations occur at the intersection of the criminal underworld and the upper world of business and politics: they hide behind a façade of businesses that look legitimate; they are enabled by an ecosystem of corruption and the protection of state-embedded actors; and they misuse sophisticated and innovative technology, such as AI, social media, fintech and VAs.

Tens of billions of dollars (USD) are generated as illicit proceeds from cyber-scam operations annually. While most of the profit is made from fraud and other illegal online businesses, proceeds are also generated from other illicit activities such as TIP, corruption and ML.

Cyber-scam operations are underpinned by a sophisticated ML service industry and crime-as-a-service providers. Cryptocurrencies and other fintech technologies, bank accounts, credit cards and cash are all misused to transfer and launder these proceeds. Hundreds of payment guarantee and over-the-counter (OTC) cryptocurrency exchanges have been set up across the key cyber-scam operation countries and in Thailand, Hong Kong, Taiwan, the Philippines, Malaysia and beyond to provide ML services to the scam syndicates. Often, compound owners themselves operate these services.

CASE STUDY - Financial Crime Arising From Cyber-Scam Centres

India's Enforcement Directorate (ED), under the Ministry of Finance, initiated an investigation based on multiple police reports registered across the country concerning cyber-enabled fraud schemes.

The investigation identified cyber-scam operations involving fake initial public offering allotments and fraudulent stock-market investment schemes promoted through deceptive mobile applications. It also uncovered impersonation schemes in which offenders posed as officials from Customs and the Anti Corruption Body to threaten victims with arrest and coerce them into transferring funds to shell companies under a purported "fund regularisation process". Parallel inquiries identified a cross-border trafficking in persons scheme in which Indian citizens were recruited through false job offers and trafficked to cyber-scam centres, where they were forced to work in call centres or to conduct cyber-scams under coercive conditions.

ED investigations revealed that the operations of cross-border trafficking syndicate operating cyber-scam compounds overseas were actively facilitated by their Indian associates who helped identify and target numerous victims. The overseas scammers coordinated with individuals in India to create digital signatures, establish shell companies, and serve as dummy Directors to open bank accounts, using fake documents sent via WhatsApp.

The ED identified a network of shell companies operating across several states, including Tamil Nadu and Karnataka, that had no genuine business activity and were registered using co-working space addresses. These entities were supported by fabricated documentation, including false bank statements. Mule bank accounts were used to receive and move illicit proceeds, which were subsequently converted into cryptocurrency and transferred overseas.

ED investigation revealed proceeds of crime totalling USD $17.51 million in illicit funds moved through various accounts, with cryptocurrency used to further conceal and transfer the money abroad. Eight arrests have been made, and the accused are currently under Judicial Custody. The financial investigations were done parallel to the TIP investigation by ED, mandated to undertake anti-money laundering investigations related to scheduled offenses including trafficking in persons.

The investigation enabled the identification of key facilitators and financial infrastructure supporting both the trafficking and fraud components of the scheme.[25]

Special economic zones

SEZs are designated areas within a country that operate under different economic regulations from the rest of the country, often offering tax benefits, relaxed trade rules, and reduced financial oversight to attract investment. However, these incentives can also create vulnerabilities that facilitate financial crime if enacted without the proportionate risk mitigation measures, such as increased opportunities for trade-based money laundering (TBML).

[25] For more information, see The Hindu (2024) *Digital arrests: ED files charge sheet, I4C issues fresh advisory.* Available at: [Digital arrests: ED files charge sheet, I4C issues fresh advisory - The Hindu.]

Casinos

FATF has long recognised casinos as vulnerable to ML, due to their high cash intensity and competitive nature.[26] A lack of effective AML controls in online casinos and gaming platforms also creates significant vulnerabilities to a range of forms of financial crime. Online gambling operations have notably been directly tied to cyber-scam centre operations in Southeast Asia in recent years, facilitating not just financial crimes but also connected crimes such as fraud and corruption.[27]

2.4 Money laundering threats in trafficking in persons

2.4.1 Money or value transfer services, including virtual assets such as cryptocurrency

Money or value transfer services (MVTS) are a range of remittance and money exchange providers. This can include large-scale providers (e.g. Western Union), or smaller unlicensed or unregulated platforms.

As these platforms tend to be more prevalent where there is a large cash-based or informal economy, they can be especially vulnerable to exploitation by criminals profiting from TIP, as well as those impacted by TIP.

Where they are not under a financial institution's structure, this also includes applications through which online payments are made (ranging from Grab to OnlyFans) and digital payment platforms, including some peer-to-peer (P2P) payment applications (e.g. PayPal). These methods offer greater anonymity and allow offenders to circumvent traditional financial monitoring mechanisms.

Some forms of MVTS have ties to particular geographic regions and are described using a variety of specific terms, such as 'hawala' or 'hundi'. In these systems, money does not physically move across borders; instead, trusted intermediaries, known as hawaladars, facilitate transfers based on a code system shared between senders and recipients, leaving minimal financial records.

[26] Financial Action Task Force (2009) *Vulnerabilities of Casinos and Gaming Sector.* Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf.coredownload.pdf

[27] United Nations Office on Drugs and Crime (2024) *Casinos, Money Laundering, Underground Banking, and Transnational Organised Crime in East and Southeast Asia: A Hidden and Accelerating Threat.* Available at: https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html

For the purposes of a 'follow-the-money' investigation, VAs can be conceptualised as MVTS. Virtual assets can transact 'on-chain'—that is, through transactions recorded on public blockchains—or 'off-chain', through transactions recorded not on the blockchain but through book-entry in the internal records of a centralised (typically custodial) service provider such as a virtual asset exchange. To analyse off-chain activity, transaction and customer identity information will need to be obtained from virtual asset service providers (VASPs). On-chain activity, on the other hand, is recorded on public ledgers and can be analysed through specialised blockchain analytics tools.

Different types of virtual assets have different features, which may affect how they are used in TIP proceeds and related financial flows. For instance:

- The virtual asset with the largest market capitalisation as of August 2025 is bitcoin (BTC). Through 2021, BTC comprised the largest share of observed financial flows to illicit addresses, and some forms of crypto-crime, such as OCSE material, remain BTC-dominated. BTC is decentralised in that there is no central issuer; seizing BTC generally requires obtaining the 'private keys' (akin to an email password) to the assets or, if assets can be traced to a centralised VASP, such as a custodial exchange, leveraging the VASP's assistance to freeze the relevant proceeds before they are cashed out.

- Stablecoins are virtual assets whose value is pegged to another asset, most commonly a fiat currency. As of end-August 2025, stablecoin market capitalisation exceeds USD $250 billion, and they account for trillions of dollars' worth of monthly value transferred on public blockchains. Their liquidity, accessibility and stable value have made them appealing for both legitimate trading, settlement and payment activities, as well as for illicit proceeds. For instance, in 2024, stablecoins accounted for the majority of observed flows to known illicit addresses on public blockchains, and they are commonly documented in the laundering of cyber-scam proceeds. However, major stablecoins today have a centralised issuer with the technical ability to freeze assets held in personal wallets.

- Some virtual assets have privacy-enhancing features which are designed to make them more challenging to trace. Monero (XMR) is one such example. While there are legitimate reasons that a user might want to obscure their transaction history, such as for financial privacy, there has also been documented use of Monero for criminal activity. However, a growing number of regulators have banned the listing of privacy coins in their jurisdiction, and major exchanges have also de-listed XMR. This constrains Monero's liquidity, making it less practical for use in large transactions.

Centralised VASPs, such as custodial exchanges, offer fiat-VA exchange services that serve as 'on-ramps' and 'off-ramps' through which fiat proceeds can enter the virtual asset ecosystem, and vice versa. Once proceeds are exchanged into virtual assets, common methods that illicit actors use to launder illicit virtual assets on-chain include:

- Use of intermediary wallets: virtual assets can be transferred across personal wallets without the involvement of an intermediary, regulated or otherwise. Personal wallets can easily be created by any entity with an internet connection. Sending or dispersing virtual assets across multiple personal wallets has been observed as a layering technique.
- Anonymity-enhancing technologies: criminals leverage services known as 'mixers' and 'tumblers' to obfuscate the origin and flow of illicit funds. By blending tainted cryptocurrencies with clean ones, these services complicate the tracing efforts of LEAs.
- Cross-chain bridges: bridges are on-chain services that enable users to move funds from one blockchain to another. These are popular tools that enhance cross-chain interoperability. However, malicious actors have also been observed leveraging cross-chain bridges as a layering mechanism by moving funds across multiple blockchains.
- P2P platforms: unregulated P2P exchanges facilitate direct transactions between individuals without the oversight of financial intermediaries. This decentralisation allows traffickers and smugglers to transfer funds across borders with reduced risk of detection.
- Decentralised Finance (DeFi) services: DeFi platforms aim to enable users to conduct basic financial transactions, such as swapping of virtual assets, lending or borrowing, in an automated way without reliance on a central intermediary. At present, many DeFi platforms are unregulated and may operate without stringent know-your-customer (KYC) protocols. Illicit actors may utilise DeFi platforms as part of the layering process, although they are not suitable as cash-out points due to the lack of integration with fiat rails.[28]

The rapid growth of the VA sector has to an extent outpaced the development of regulatory frameworks, creating gaps that traffickers can exploit. For instance, unregulated VASPs including certain over-the-counter services and peer-to-peer (P2P) transactions may facilitate transactions without meaningful know-your-customer (KYC) measures, enabling criminal actors the ability to place, layer and cash out illicit virtual assets. For instance, one laundering typology observed in the laundering of cyber scam proceeds is the utilisation of so-called "Black U" services – illicit platforms, primarily operating through Chinese-language Telegram channels, facilitating the swapping of USDT obtained through illicit means for clean funds. Since 2022, "Black U" laundering services have processed billions of USD worth of virtual asset inflows.

[28] Financial Crimes Enforcement Network (2024) *FinCEN Sees Increase in BSA Reporting Involving the Use of Convertible Virtual Currency for Online Child Sexual Exploitation and Human Trafficking.* Available at: https://www.fincen.gov/news/news-releases/fincen-sees-increase-bsa-reporting-involving-use-convertible-virtual-currency; Chainalysis (2024) *Money Laundering and Cryptocurrency: Trends and New Techniques for Detection and Investigation.* Available at: https://airant.org/wp-content/uploads/2024/07/Report_-Money_laundering_and_Cryptocurrency.pdf

FATF found in April 2025 that 70 per cent of jurisdictions which had been assessed for compliance with the FATF Standards for VAs and VASPs were found to be partially compliant or non-compliant.[29] Jurisdictional discrepancies can complicate international cooperation efforts, while the limited capacity of jurisdictions to identify and investigate such activity can further hinder effective counter-trafficking efforts.

These jurisdictional discrepancies and capacity constraints can also extend to certain types of P2P activity, specifically VA transfers conducted without the use or involvement of a VASP or other obliged entity (e.g. VA transfers between two unhosted wallets whose users are acting on their own behalf). Unregulated P2P exchanges facilitate direct transactions between individuals without the oversight of financial intermediaries. This decentralisation allows traffickers and smugglers to transfer funds across borders with reduced risk of detection.

2.4.2 Designated non-financial businesses and professions

Designated non-financial businesses and professions (DNFBPs) can be used (knowingly or unknowingly) to facilitate money laundering, e.g. in creating complex legal persons and arrangements to conceal the beneficial owner or the origin of funds.

Money Laundering Risks In Designated Non-Financial Businesses and Professions

DNFBP Sector	**Examples**
Real estate agents Lawyers Accountants Trust and company service providers Notaries	Property purchases are often used to launder large sums of illicit funds, particularly in high-value real estate markets, to integrate illicit proceeds into the economy. This can include making purchases in cash, over- or under-valuing properties, or using complex/opaque legal persons to obscure the beneficial owner.
Casinos	In-person and online casinos and gambling companies can be used in a variety of ways for money laundering. This can include purchasing casino chips and cashing them out (appearing as legitimate earnings)[30] or purchasing in-game points or prizes. Many online platforms operate with minimal KYC requirements, allowing traffickers to register accounts under false identities. 'Junkets' (overseas tours for high-wealth gamblers for the purpose of gambling) and high-roller casinos.

29 Financial Action Task Force (2025) *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers.* Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

30 United Nations Office on Drugs and Crime (2024) *Casinos, Money Laundering, Underground Banking, and Transnational Organised Crime in East and Southeast Asia: A Hidden and Accelerating Threat.* Available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

SECTION 3

BUILDING BLOCKS OF AN EFFECTIVE AND HOLISTIC FOLLOW-THE-MONEY APPROACH TO TIP

Effective TIP responses require collaboration among government, civil society and the private sector. There are several foundational building blocks to support effective follow-the-money approaches for TIP, at all stages (prevention, identification, investigation, asset tracing/confiscation and prosecution).

These are:

- Legal and regulatory frameworks, including sufficient AML, international cooperation and asset confiscation regimes.
- Establishing competent authorities with sufficient domestic coordination mechanisms.
- Conducting financial investigations.
- Stakeholder engagement with public sector, private sector and civil society.
- Formal and informal international cooperation.

3.1 Legal and regulatory frameworks

National responses to TIP are defined by legal and regulatory frameworks that outline stakeholder obligations and responsibilities. These stakeholders typically include government agencies, private sector entities and civil society actors working to prevent, protect, investigate and prosecute TIP cases.

The FATF Standards provide jurisdictions with the core legal and regulatory frameworks necessary to effectively identify, investigate and prosecute ML.

3.1.1 Anti-money laundering frameworks

Financial crime investigations, including those linked to predicate crimes such as TIP, are a crucial component of an effective AML regime. National AML regimes are regularly reviewed for compliance with the global minimum requirements, as set by the FATF. These global standards (known as the 'FATF Standards') cover a range of vital areas for an effective AML regime, and provide critical foundations for a country to effectively leverage 'follow-the-money' approaches in TIP investigations.

Relevant requirements included in the FATF Standards include:

- Identifying, assessing and understanding money laundering and predicate crime (such as TIP) risks.
- Effective coordination among competent authorities.
- Timely and effective international cooperation.
- Supervising 'regulated entities' (such as financial institutions, MVTS and 'gatekeeper' professions such as lawyers, accountants and real estate professionals) for proportionate money laundering risk mitigation measures—this includes requiring entities to report on 'suspicious' activity and transactions.
- Identifying, investigating and prosecuting money laundering (and predicate crime) activity in line with the jurisdiction's risk profile.
- Suspending or withholding transactions.
- Identifying, tracing, freezing/seizing and confiscating criminal property and property of corresponding value.

Regardless of how it is achieved, a robust AML regime is an effective tool in combating trafficking in persons. Across the Bali Process region, legislative and regulatory approaches to tackle TIP and money laundering vary. Gaps in these regimes (such as unregulated MVTS) can decrease the effectiveness of a jurisdiction's AML regime and increase opportunities for exploitation for TIP.

- In the United States, Section 1592 within Chapter 77 of Part 1 of the 18th Title of the US Code (18 USC § 1592) addresses interstate and foreign travel or transportation in aid of racketeering enterprises,[31] with specific application to TIP offences. Key provisions include criminalising acts that deprive trafficking victims of identity documents for the purpose of further exploitation and addressing cross- jurisdictional trafficking. Section 1592 is triggered by any financial transactions related to trafficking, including electronic funds transfers. The statute enables law enforcement to intervene in ongoing trafficking operations and facilitates the building of federal TIP cases while separating alleged perpetrators from potential TIP victims.
- In the Republic of Indonesia, Law No. 8 of 2011 on Money Laundering Prevention and Eradication recognises TIP as one of the predicate offences of ML. Articles 3, 4, 5, and 6 of Law No. 8 of 2011 describe the scope of ML as any act committed by an individual or corporation to place, transfer, conceal, disguise, receive, or take control of assets known or reasonably suspected to be derived from a criminal offence, with the purpose of hiding or disguising the true origin, source, location, allocation, or actual ownership of such assets. These acts may be carried out through various means, whether for personal or corporate benefit, insofar as they provide an advantage to the corporation or are carried out under the instruction of the corporation's controlling personnel. Specifically for TIP prevention, countermeasures, and eradication, the Republic of Indonesia has Law No. 21 of 2007.

[31] The US Code is the official codification of all US statutes.

- In India, the 2002 Prevention of Money Laundering Act (PMLA) designates the Enforcement Directorate as the primary authority responsible for preventing money laundering and for tracing, freezing, seizing, and confiscating property derived from, or involved in, money-laundering offences. Under section 8(8) of the PMLA, Special Courts may direct that confiscated property be restored to victims who have suffered losses as a result of money-laundering offences. These measures may be applied in cases where TIP constitutes a predicate offence, enabling asset recovery to complement TIP prosecutions.

India's Value-Based and Non-Conviction-Based Confiscation Under the PMLA

A key feature of the PMLA is the availability of value-based confiscation, in line with FATF Recommendation 4. Under these provisions, assets of an equivalent value to the proceeds of crime may be provisionally attached or confiscated, even where the original illicit proceeds are no longer available. Property subject to attachment is not limited to assets acquired after the commission of the predicate offence; assets acquired prior to the offence, and even prior to the enactment of the PMLA, may also be subject to provisional measures or confiscation.

The calculation of criminal benefit generally involves assessing the total financial gain derived from illegal activity, including direct and indirect profits, savings, and other economic advantages. Where property has been acquired below market value, benefit is calculated based on the fair market value of the asset. Asset valuations are conducted by official valuation panels based on case-specific facts.

The PMLA, together with the Fugitive Economic Offenders Act, 2018, also enables non-conviction-based confiscation, including in circumstances where an accused person has fled India to evade prosecution or refuses to return to face legal proceedings.

3.1.2 Asset recovery frameworks—proceeds of crime and criminal assets confiscation

The FATF Standards also set out the minimum expectations for an effective transnational asset recovery framework that leads to permanent deprivation of criminal property (Recommendations 4 and 38, Immediate Outcomes 2 and 8). This includes mechanisms for provisional and permanent measures to freeze, seize and confiscate criminal property and property of corresponding value.

In accordance with the fundamental principles of its domestic law, a jurisdiction should also ensure that, where possible, legislation contains measures that offer victims of TIP the possibility of obtaining compensation for damage suffered, as well as consider implementing measures to support victim rehabilitation.[32] Jurisdictions should also consider the approach of redirecting confiscated proceeds of TIP to such endeavours, if appropriate and in accordance with their own domestic laws. Such an approach ensures that criminal proceeds are used responsibly and serve to benefit exploited individuals.

Some BPMS report lengthy delays and hefty administrative burdens in pursuing conviction-based confiscation (CBC) actions. As an acceptable alternative that complements traditional CBC regimes, non-conviction-based confiscation (NCBC) frameworks enable law enforcement to seek confiscation in the absence of a criminal conviction, but where the link to criminality can be demonstrated to the civil standard of proof.

In addition to understanding domestic laws, cooperation with key foreign partners is important as it can facilitate the identification, tracing, freezing, seizing and confiscation of assets and subsequent repatriation of part or all of the property or funds to the jurisdiction impacted by the criminal offending.

NCBC in Australia

- Australia uses a civil NCBC scheme under its Proceeds of Crime Act 2002 (POCA).
- The Australian Federal Police (AFP) can apply to the relevant court seeking a provisional order (e.g. freezing order, restraining order) or permanent order (e.g. forfeiture and confiscation orders and unexplained wealth orders) against identified persons or persons at large and over property of all forms.
    - The court is required to make such an order if there are reasonable grounds to suspect that the property is proceeds from an indictable offence or is wholly or partly an instrument of a serious offence.
    - Where the owner of the property cannot be identified, but the court is still satisfied that the property is linked to criminality, the POCA enables orders to be made directly against the property.
- The funds realised from the liquidation of confiscated assets are deposited into the Confiscated Assets Account (CAA), managed by the Australian Financial Security Authority.
- Funds deposited into the CAA are used to benefit the community through crime prevention, intervention or diversion programs or other law enforcement or community related initiatives.

[32] United Nations (2000) *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime*. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons

CASE STUDY - EUROPOL - Operation Global Chain

The following case study illustrates the value of multi-agency and regional cooperation between law enforcement officers and FIUs.[33]

Operation Global Chain, led by EUROPOL, was a six-day multi-national, multi-agency TIP operation in June 2025, which resulted in the safeguarding of 1,194 potential victims. The operation aimed to detect and disrupt High-Value-Targets and organised crime groups as well as safeguarding victims, seizing criminal assets and generating follow-up investigations. Law enforcement officers from 52 countries, including Thailand and Vietnam, targeted organised criminal gangs trafficking people for the purposes of sexual exploitation, forced criminality and begging. In addition to the arrest of 158 traffickers, significant seizures of cash, drugs and firearms were made:

- **EUR €277,669 in cash**
- **1 tonne of cannabis**
- **899 units of other narcotics**
- **30 firearms**
- **15 explosive components**
- **5 real estate properties**

[33] Europol (2025) *158 Human Traffickers Arrested and 1,194 Victims Safeguarded in Global Operation*. Available at: https://www.europol.europa.eu/media-press/newsroom/news/158-human-traffickers-arrested-and-1-194-victims-safeguarded-in-global-operation

3.1.3 International cooperation frameworks

Countries should ensure an enabling framework for regional and international cooperation for matters relating to financial crime and TIP, as contemplated under Recommendation 40 of the FATF Standards.

International cooperation can take many forms, including Mutual Legal Assistance (MLA) and extradition as examples of 'formal' international cooperation. Outside of these 'formal' mechanisms, many agencies (especially law enforcement) can leverage 'informal' mechanisms, such as joint taskforces with foreign counterparts, information exchanges or even basic correspondence. In line with international instruments and the FATF Standards (Immediate Outcome 2), countries should ensure their legal and regulatory framework allows rapid, constructive and effective assistance, including in recognising and enforcing foreign asset recovery orders (regardless of whether they arose from conviction-based or non-conviction-based proceedings).

Legal and regulatory frameworks, including operating procedures and policies for competent authorities, should also enable informal international cooperation. This can include protocols for timely exchange of information between FIUs, banks and LEAs, or engaging in a range of regional exercises and initiatives. For example, the Asset Recovery Inter-Agency Networks (ARINs) are informal regional networks bringing together LEAs working to trace, freeze, seize and confiscate assets. The Egmont Group and International Criminal Police Organization (INTERPOL) provide additional platforms for secure informal information exchange and operational coordination on asset recovery. These mechanisms are examined in more detail in Section 5.

Regional initiatives, such as the ASEAN Multi-Sectoral Work Plan against TIP,[34] are examples of collaborative efforts to implement the ASEAN Convention against Trafficking in Persons (ACTIP).

Given the transnational nature of TIP and of ML generally, an important foundation to strengthening domestic legal and regulatory frameworks is to sign and ratify important international instruments, including:

- The United Nations Convention Against Transnational Organized Crime (UNTOC) (the Palermo Convention).
    - including the Palermo Protocol (Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children).
- The United Nations Convention Against Corruption (UNCAC) (the Merida Convention).
- The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention).

Full implementation of these international instruments provides a strong legal basis for various elements of an AML regime (e.g. asset recovery and international cooperation), as required under the FATF Standards (Recommendation 36).

[34] Association of Southeast Asian Nations (2023) *ASEAN Multi-Sectoral Work Plan against Trafficking in Persons 2023–2028*. Available at: https://asean.org/wp-content/uploads/2023/10/Adopted-ASEAN-Multi-Sectoral-Work-Plan-Against-TIP-2023-2028-as-of-08-21-23.pdf

CASE STUDY - India's "1930 Take Down System"

India's "1930 Take Down System" is a structured framework and platform for addressing various cyber-enabled crimes, including OCSE. Victims can report these offences through the cybercrime portal (www.cybercrime.gov.in) or the dedicated 1930 helpline, after which the reports are processed through the portal. All reports are sent to cyberpolice.nic.in, which connects to the LEAs dashboard for further investigation and action. India's LEAs, using this dashboard, coordinate take-down requests of harmful content, reported by specially focused bots on social media and other online platforms. Tips from other sources, including the National Center for Missing and Exploited Children (NCMEC), which operates a CyberTipline receiving reports of online child sexual exploitation from electronic service providers and the public, and financial investigation agencies within India and abroad, are added and analysed through AI-based filtering tools, helping LEAs identify pertinent cases. These cases are then stored in the Cybersexual Offender Database, which assists in tracking known offenders and preventing recurrences. This data is also integrated into a broader dashboard for real-time monitoring, mapping, and managing cases across regions, enhancing the efficiency of response and coordination by LEAs.[35]

3.1.4 Measures for regulated entities

As part of an effective legal and regulatory framework, countries should ensure their regime imposes proportionate obligations on reporting entities (including financial institutions, DNFBPs and VASPs). This is important for financial investigations as it ensures that LEAs and FIUs have access to relevant financial information, such as Suspicious Transaction Reports (STRs) and Threshold Transaction Reports/Currency Transaction Reports (TTRs/CTRs) from 'regulated entities', such as banks, MVTS and DNFBPs.

It is important to emphasise that the FATF Standards are underpinned by an RBA, which encourages the targeting of resources in a way that is proportionate to the identified risk. Countries should ensure their legal and regulatory framework meets key compliance obligations under the FATF Standards that support the identification and investigation of TIP, including:

35 Financial Action Task Force (2025) *Detecting, Disrupting and Investigating Online Child Sexual Exploitation.* Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Online%20Child%20Sexual%20Exploitation%20Report.pdf.coredownload.inline.pdf

- **Customer Due Diligence (CDD) and KYC Requirements:** Under Recommendations 10 and 22, regulated entities must apply CDD requirements that are proportionate to the risk posed by the customer. This includes implementing practices to identify and verify customers, including the 'beneficial owner' (where the customer is a legal person/arrangement).
    - Where the ML risks are higher (e.g. as identified in the regulated entity's institutional risk assessment), or there is a suspicion of ML, regulated entities should be required to perform Enhanced Due Diligence (EDD).
    - Likewise, in identified lower risk scenarios, regulated entities should be allowed and encouraged to use simplified measures, including Simplified Due Diligence (SDD), to ensure an appropriate implementation of the RBA which fosters financial inclusion.

- **Reporting of suspicious transactions:** Under Recommendation 20, regulated entities must submit a report to the FIU if they suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity, including TIP.

- **Tipping-off offences:** Under Recommendation 21, regulated entities (including their directors, officers and employees) should be prohibited from disclosing information that would 'tip-off' someone engaging in financial crime.

- **Beneficial ownership transparency:** Under Recommendations 24 and 25, countries should ensure their legal frameworks require the collection of basic and beneficial ownership information that is adequate, accurate and up to date. This information should be accessible by competent authorities in a timely manner.

- **Cross-border reporting and international cooperation:** Financial institutions and regulatory bodies must share intelligence on suspicious financial flows across jurisdictions, particularly within high-risk regions.

- **MVTS:** Under Recommendation 14, all individuals or legal persons who provide MVTS should be required to be licensed or registered.

3.1.5 Supervisor responsibilities

To ensure and strengthen compliance by regulated entities, supervisors should provide clear guidance and outreach relevant to TIP. Supervisors should provide regular and constructive feedback to regulated entities regarding common TIP typologies and indicators, including when undertaking supervisory activities.

Depending on the risk and context, competent authorities should consider applying dissuasive and proportionate sanctions for those in breach of the legal and regulatory frameworks to enhance TIP-related outcomes. Sanctions may include fines, licence revocations, and other enforcement actions to deter non-compliance. For example, unlicensed or unregistered MVTS providers should first be brought into the jurisdiction's licensing or registration system; however, those who refuse to comply, or otherwise facilitate the exploitation of their network for TIP and financial crime, should be appropriately sanctioned by the competent authorities to limit vulnerabilities.

Such activities should be permitted in the country's legal and regulatory framework, in accordance with Recommendations 26–28 and 34 of the FATF Standards.

CASE STUDY - Pakistan's Anti-Money Laundering Act and Anti-Terrorism Act

Pakistan has undertaken significant measures to combat money laundering and the financing of terrorism, particularly in relation to TIP and people smuggling. Central to these efforts is the Anti-Money Laundering Act (AMLA) of 2010, which criminalises money laundering and establishes procedures for the investigation and prosecution of such offences. Complementing this is the Anti-Terrorism Act (ATA) of 1997, addressing offences related to terrorism financing.

Despite these advancements, challenges persist, particularly concerning the informal financial sector and unregulated remittance services such as hawala, which are susceptible to exploitation for TIP-related payments. To address these issues, Pakistan continues to enhance its regulatory framework, improve inter-agency coordination, and engage in capacity-building initiatives. Collaborations with international organisations and adherence to global standards set by bodies such as the FATF remain integral to Pakistan's strategy in combating money laundering and terrorist financing.

3.2 Establishing competent authorities with sufficient domestic coordination mechanisms

Investigating TIP through financial investigations requires a whole-of-government response. Responses should involve numerous agencies that can intervene at various stages of the criminal supply chain to prevent, investigate and prosecute TIP-related cases. The agencies described below often take a leading role in these efforts, however, this does not mean that the work of other agencies is less important.

Collecting statistics can be a valuable way to measure success, ensure an RBA that responds to higher risks, and inform domestic cooperation.[36]

[36] Information to identify and understand the key AML authorities in each country is readily available in the most recent FATF Mutual Evaluation. Available at: https://www.fatf-gafi.org/en/topics/mutual-evaluations.html

3.2.1 Financial Intelligence Units

FIUs should be established in accordance with Recommendation 29 of the FATF Standards. FIUs play a key role in facilitating an effective 'follow-the-money' approach, as they receive information from a range of sources (including Suspicious Transaction Reports (STRs) and Transaction Threshold Reports (TTRs) from reporting entities, collect and analyse the information and disseminate financial intelligence to LEAs to support investigations. The diagram below shows the flow of information to and from a FIU.

Figure 2: The financial intelligence cycle, showing how reporting entities submit transaction reports to FIUs.

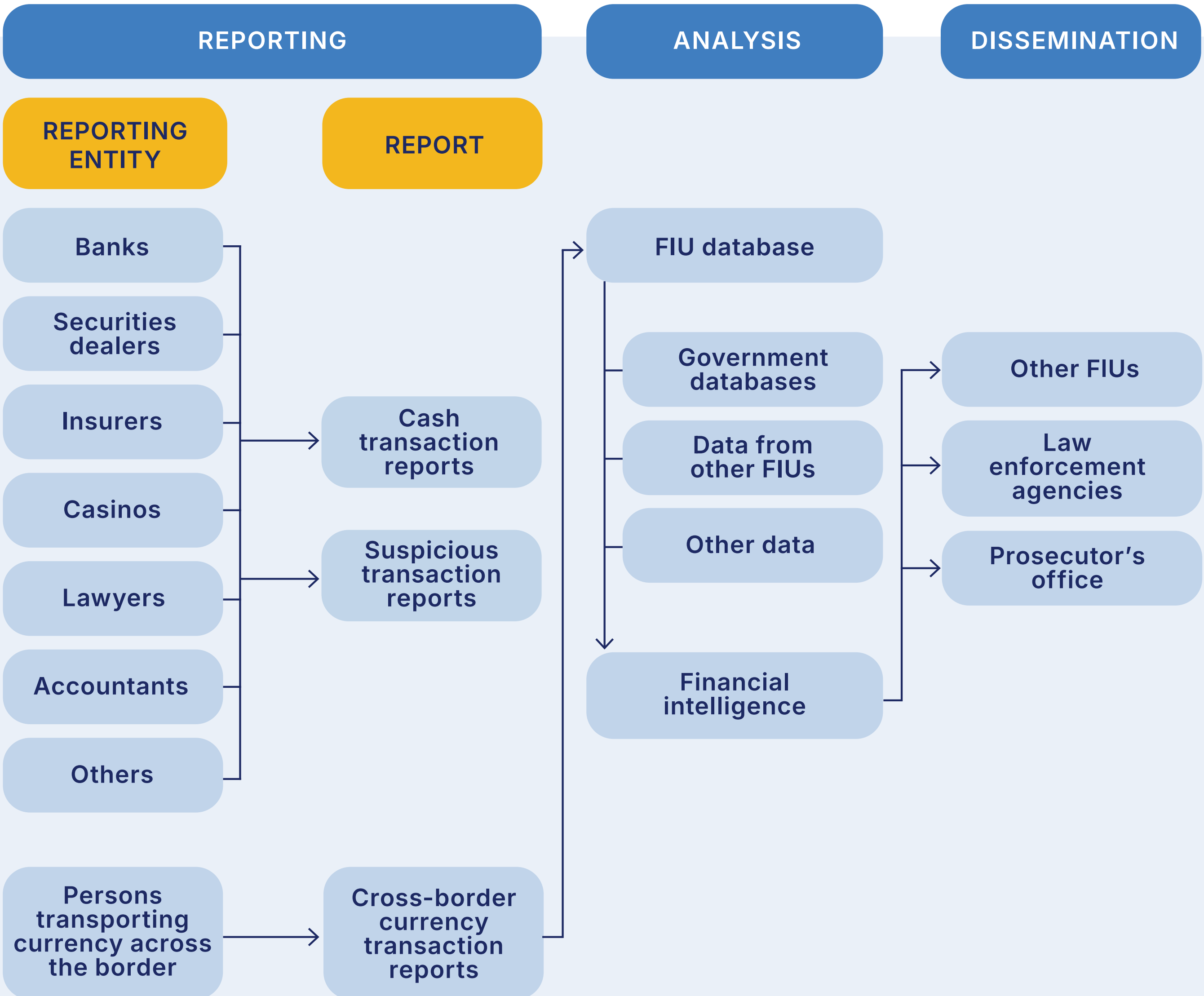


Diagram from: Financial Intelligence Units: An Overview, IMF World Bank, 2004

FIUs play a pivotal role in detecting and disrupting illicit financial flows linked to TIP by collecting and analysing financial data from reporting entities to identify patterns indicative of criminal activity. This includes recognising behavioural red flags such as frequent small cash deposits, rapid movement of funds across accounts, and transactions inconsistent with a customer's known profile.

FIU analysis is strengthened by cross-referencing other law enforcement records and databases, enabling the development of financial intelligence that supports law enforcement investigations.

Timely dissemination of financial intelligence enables law enforcement to take immediate investigative actions, while international cooperation among FIUs helps uncover cross-border criminal networks. The Egmont Group's operational guidance highlights the importance of FIUs having access to a broad range of financial, administrative, and law enforcement information to conduct in-depth analyses and support investigations.[37]

Though detailed below in 'Stakeholder engagement', it is relevant to highlight here that, in addition to coordination among competent authorities, FIUs often also serve as an important intermediary between the private and public sectors, aiding in the early identification and prevention of emerging financial risks linked to TIP.

Where an FIU does not have investigative functions, domestic coordination and mutual feedback with LEAs is even more important to effective TIP investigations.

3.2.2 Law enforcement agencies

LEAs often lead TIP investigations, as they are responsible for apprehending criminals and disrupting illegal activities. Each country's operational framework and LEA landscape differs, with some systems comprising several LEAs, including national police services and specialised departments focusing on serious and organised crime.

In addition, multinational LEAs, such as the INTERPOL and the Organisation of the ASEAN Chiefs of National Police (ASEANAPOL), facilitate collaboration and provide investigative insights into TIP crimes. They provide member countries with tools and resources (e.g. criminal and victim databases) and issue notices about wanted traffickers or missing persons. This helps to bridge jurisdictional gaps and enhance collaboration.

[37] Egmont Group (2013, revised 2017) *Egmont Group of Financial Intelligence Units Operational Guide for FIU Activities and the Exchange of Information.* Available at: https://egmontgroup.org/wp-content/uploads/2021/09/Egmont_Group_of_Financial_Intelligence_Units_Operational_Guidance_for_FIU_Activities_and_the_Exchange_of_Information.pdf

While LEAs globally have dedicated significant resources to a TIP response, most activities focus on reactive measures (i.e. focused primarily on the traffickers, and only focusing on victims after they are exploited) and less on prevention efforts. Using a 'follow-the-money' approach enables LEAs to proactively identify and prevent TIP, rather than relying on traditional reactive approaches.

Key challenges highlighted by law enforcement in the Bali Process region include:

- Difficulties handling electronic evidence;[38] in particular, some report limited capacity for investigating blockchain-related transactions.
- High turnover of trained personnel; although some law enforcement personnel have received significant training through collaborative efforts, some leverage this training to get new jobs, utilise skills for other operational priorities or request to be transferred to other units for career progression.
- Limited regional collaboration and information sharing.
- Resource constraints, in particular, low human-resource and infrastructure capacity including computerised and analytical tools.

3.2.3 Prosecutors and the judiciary

To ensure an effective whole-of-government response to both TIP and financial crime investigations, it is important not to 'fall down at the last hurdle' and ignore the importance of the judiciary. This includes the courts, judges and prosecutors.

Despite their critical role, experts have raised concerns about the judiciary's knowledge and understanding of TIP-related crimes. For example, online offences are often regarded as less serious than physical exploitation. Judges also report having limited access to data on the latest TIP trends. Additionally, the increasing prevalence of digital payment methods complicates evidence-gathering, investigation efforts and the evaluation of evidence, particularly where exploitation takes place across multiple jurisdictions.

The judiciary interacts with TIP and financial crime investigations at various stages, including in granting provisional orders (e.g. freezing/seizing orders) all the way through to the trial of alleged criminals and the making of final confiscation orders. It is therefore fundamental to an effective regime to ensure that the capability of the judiciary is enhanced along with that of other competent authorities to ensure a well-informed approach to TIP and financial crime proceedings.

To enhance the judiciary's capacity in combating TIP, it is crucial to educate prosecutors, judges and lawmakers about the typologies for TIP offending and ML, and the individual and societal harms from TIP in various digital and physical forms.

[38] There may also be challenges around recruitment and training of forensic examiners, who are required to investigate digital devices for evidence.

Australia's Criminal Assets Confiscation Taskforce and the Proceeds of Crime Act

Australia's Proceeds of Crime Act (POCA) enables a coordinated, proactive approach to asset confiscation, in part by establishing the Criminal Assets Confiscation Taskforce (CACT) within the Australian Federal Police (AFP). The CACT has a nationwide presence with expertise provided by police officers, financial intelligence, financial accounting specialists and in-house litigators. This helps prioritise asset confiscation alongside criminal investigations.

The CACT is the primary authority for investigating and conducting asset confiscation litigation in collaboration with various domestic and international LEAs. The CACT integrates resources and expertise from multiple Australian agencies, including the AFP, the Australian Criminal Intelligence Commission, the Australian Taxation Office, AUSTRAC (Australia's financial intelligence unit) and the Australian Border Force.

Consistent with the principal objects of the POCA, the CACT seeks to deprive persons and criminal groups of the proceeds, instruments and benefits of their offending, to punish and deter persons from breaching laws, and to undermine the profitability of criminal enterprises and prevent the reinvestment of illicit property into further criminal activities.

3.2.4 Domestic coordination mechanisms

In accordance with Recommendation 2 of the FATF Standards, an effective AML regime hinges upon regular coordination and cooperation among relevant competent authorities, such as the policy-makers, FIU, LEAs, supervisors etc.

Fundamentally, FIUs and LEAs should maintain open communication to enhance multi-agency collaboration and coordination in investigations. Depending on a country's risk and context, and legal/regulatory framework, the ways in which competent authorities cooperate and coordinate can differ. This can be achieved informally through officer-to-officer engagement, or by establishing formal coordination mechanisms such as:

- Centralised coordination units: Creating dedicated units that serve as focal points for TIP cases ensures streamlined communication and resource allocation. These units can manage case information, coordinate with international counterparts, and oversee the progress of investigations.

- Joint Investigative Teams (JITs)/taskforces: Establishing JITs to investigate TIP and financial crime can be an effective use of shared resources and expertise to more quickly achieve tangible outcomes. In addition to domestic authorities, this can be expanded to involve international agencies (Recommendation 40).

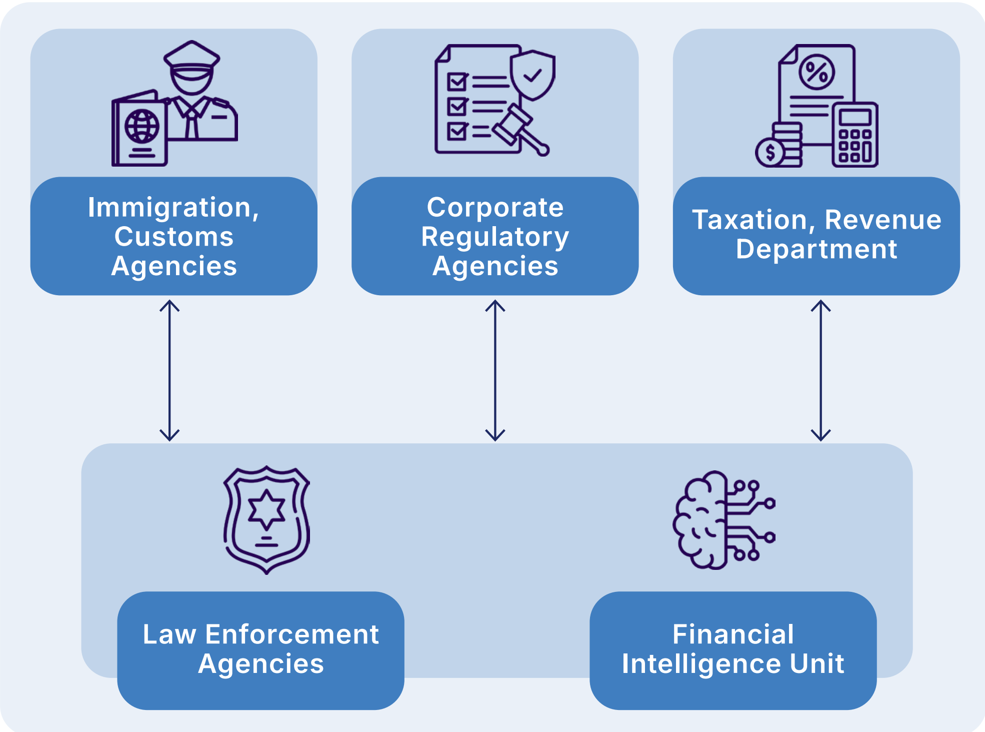
- Regular inter-agency meetings: Holding routine meetings between LEAs, FIUs, and other relevant competent authorities fosters information sharing, updates on ongoing cases, and the development of joint strategies to address emerging threats.

Enhancing domestic cooperation and coordination mechanisms between FIUs, LEAs and other competent authorities can significantly enhance investigations, including those harnessing new technologies or with significant cross-border elements.

There is a clear need to continue building FIU and LEA capacity and technical skills for 'follow-the-money' investigations—including through regional P2P trainings and exchange.

In addition to case coordination, FIUs and LEAs should regularly seek and provide feedback on the value of financial intelligence products, the outcome of investigations, the needs of LEAs, etc. to continually improve the quality of financial intelligence products.

Figure 3. Cooperation on financial investigations between different domestic agencies.



3.2.5 Domestic partners and agencies

Where possible, investigations into TIP should include domestic partners and agencies, including immigration departments, to enhance enquiries into the movement of trafficked victims. As trafficking involves the transportation and transfer of victims, usually across international borders, immigration systems may contain valuable information for investigators relating to the movement of trafficked persons, such as:

- Visa and work permit documentation and details about the entities who have assisted in the visa application process.
- Payments for fees, visas and transport.
- Information about previous residence, study, employment and associates/family members.

Immigration departments, including officers with specialist knowledge and experience, may have insights and contacts in the travel industry, at airports and at other land/sea border crossings, which can add critical details to enhance a 'follow-the-money' approach to TIP investigations.

Other domestic government agencies, such as revenue, taxation and corporate regulatory bodies, may have access to additional information and data, which can assist investigators in identifying key enablers and offenders in a TIP network.

Just as critically, when undertaking a criminal investigation, domestic partners and agencies may have a range of powers which can complement those of traditional LEAs. These powers can be leveraged to detect, investigate and prosecute criminal activity.

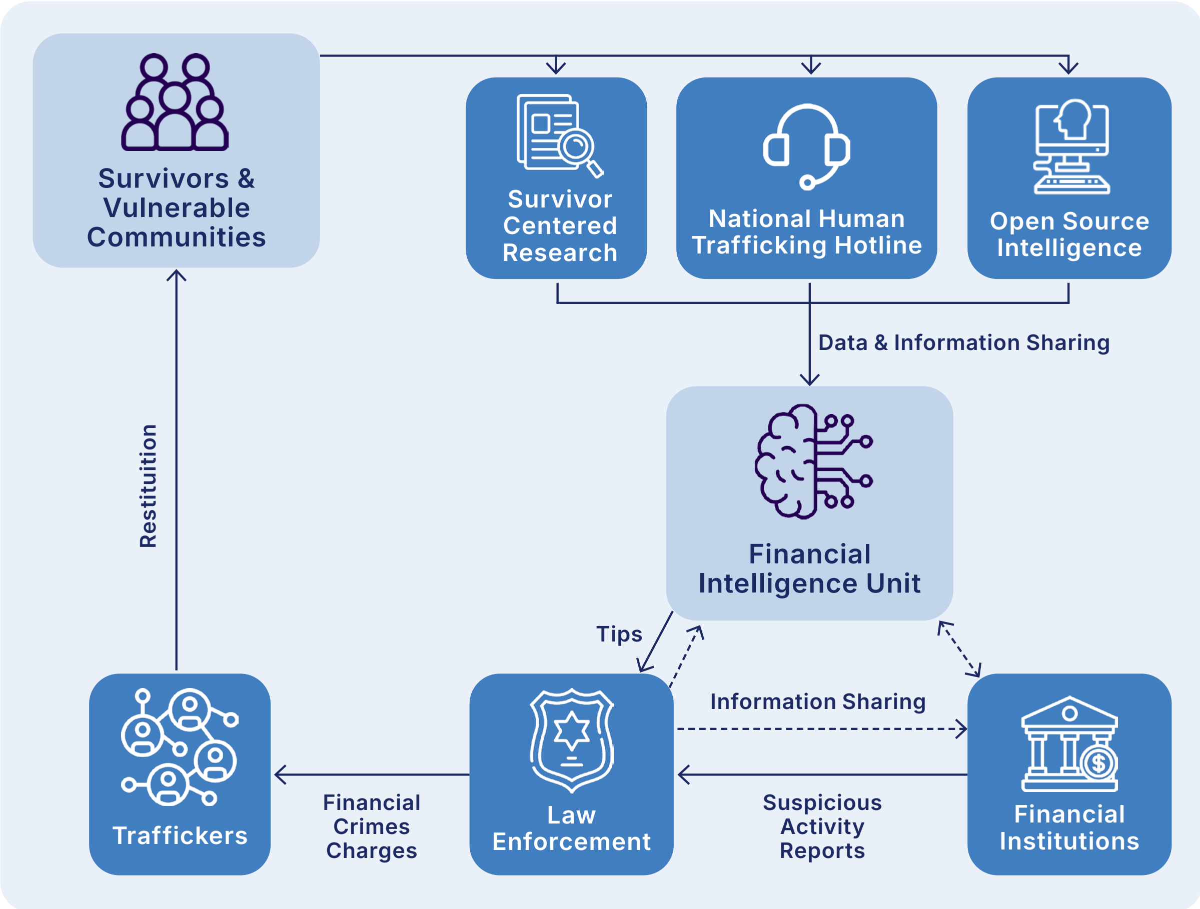
3.3 Conducting financial investigations

There are two primary avenues of inquiry in TIP financial investigations: the flow of illicit funds laundered by traffickers, and the flow of funds from trafficked persons. Financial transaction activity from trafficked persons includes remittances to family members in countries of origin, often sent through money transfer services or bank accounts. Victims may also make payments to criminal actors for the purpose of paying debts. Investigators need to be aware that financial flows from trafficking in persons may contain a commingling of licit and illicit funds and that this may be difficult to disentangle.

These investigations primarily start in one of two ways:

- The LEA initiates an investigation of a TIP case, which can be triggered through financial intelligence from the FIU or other methods of identifying criminal activity; or
- The FIU initiates an investigation based on financial intelligence, such as an STR.

Figure 4. The information-sharing networks that exist between FIUs and relevant institutions and groups.



Regardless of which government department or agency initiates an investigation, 'following the money' remains a key challenge in TIP investigations.

A further challenge identified across the Bali Process region is the timing of financial investigations in TIP cases. Financial investigations are often conducted after the conclusion of the primary TIP investigation. This enables the defendants to hide or divert the proceeds of their crime. Financial investigations should be carried out simultaneously with TIP investigations with 'follow-the–money' strategies integrated from the outset of the case. This includes obtaining interim orders, such as freezing or seizing orders, in relation to property, but also obtaining evidence preservation orders (production of financial and property-tracking documents) to mitigate the risk of dissipation of assets and evidence destruction.

It is good practice to establish parallel financial analysis as part of the overall TIP investigation. Such investigations complement traditional law enforcement efforts by simultaneously targeting the economic foundations of these crimes.

For additional information, the FATF provides thematic guidance on financial investigations related to TIP cases.[39]

Ethical considerations in TIP investigations

Protection of victims and prevention of re-traumatisation is crucial in any TIP investigation. This should be done through a victim-centred approach which places the survivor's safety, autonomy and mental health at the forefront. Safe interview environments should be created where victims can express their concerns, and interviewers should be trained in trauma-informed practices to recognise the complex emotional and psychological impacts of trafficking. In addition, victims' dignity and privacy should be protected at all steps of the process.[40]

3.3.1 Identifying the financial footprints of traffickers

The initial step involves detecting the financial activities associated with TIP. This requires a comprehensive understanding of the financial behaviours typical of traffickers and their victims. When monitoring transactions for AML purposes, certain financial patterns can serve as an indicator of potential TIP-related activities for LEAs and FIUs.

When conducting an investigation, keep in mind the full spectrum of payments, from financial flows of victims (i.e. scam victims, TIP victims) to larger scale laundering and reinvestment in the formal economy. These flows can also be useful to identify syndicated or network behaviour and actors.

39 Financial Action Task Force (2018) *Financial Flows from Human Trafficking*. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Human-Trafficking-2018.pdf.coredownload.inline.pdf; Financial Action Task Force (2023a) *Recovering International Proceeds of Crime through Inter-Agency Networks*. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/recovering-international-proceeds-crime-inter-agency-networks.html; Financial Action Task Force (2023b) *Illicit Financial Flows from Cyber-enabled Fraud*. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html; Financial Action Task Force (2023c) *Financial Action Task Force–INTERPOL Partnership: Igniting Global Change to Take the Profit Out of Crime*. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/FATF-Interpol-partnership.html

40 To support practitioners in the ethical considerations of trafficking in persons investigations, the Nexus Institute and the Regional Support Office of the Bali Process have developed a series of Practitioner Guides available in English, Bahasa Indonesia, Bahasa Malaysia, Vietnamese and Thai. Available at: https://nexusinstitute.net/room/practitioner-guide-series-available-in-indonesian-malaysian-and-vietnamese-january-2022/

Financial red flag indicators linked to trafficking in persons: Cash, accounts, and financial institutions

Financial indicator	Examples	Possibly indicative of
Unusual cash transactions	▶ Cash deposits or withdrawals occurring frequently between 10 p.m. and 6 a.m. ▶ Multiple small cash deposits conducted at different bank branches or ATMs, often across different cities or provinces. ▶ Large cash deposits followed by rapid withdrawals, bill payments, or electronic transfers to third parties. ▶ Account funded primarily via third-party cash transactions.	Trafficking for the purpose of sexual exploitation
Unusual location-based activities	▶ Repeated hotel transactions with rounded sums. ▶ A single individual booking multiple rooms at the same hotel for the same dates. ▶ Hotel transactions followed by refunds for the same amount, potentially to obscure the financial trail. ▶ Hotel accommodations booked using pre-authorised credit cards but paid in cash upon arrival. ▶ Frequent gambling activity and cash withdrawals from ATMs located in or near casinos.	Trafficking for the purpose of sexual exploitation
Suspicious account activities (individual)	▶ Personal accounts receiving frequent deposits but maintaining low balances, with no evidence of normal personal expenditures. ▶ Accounts functioning as 'funnel accounts', receiving deposits from multiple locations that do not correspond with the account holder's stated place of residence or business.	Trafficking for the purpose of sexual exploitation

	▶ The suspected victim is accompanied into a bank by a third-party individual who speaks on their behalf, or appears coercive, aggressive or is withholding documents or funds. ▶ Email money transfers listing alternative names in brackets, e.g. jane@example.com (Bambi), suggesting alias use to conceal identities. ▶ 'Structuring' of transactions, often to below the jurisdiction's reporting threshold (USD $10,000/ EUR €10,000 under the FATF Standards).	
'Money mules'	▶ Unrelated third parties sending email money transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient or no stated purpose for the transfers. ▶ Account shows pass-through activity: receives funds (often from multiple third parties) and quickly forwards/withdraws most or all funds, maintaining a consistently low balance. ▶ Account-holder appears directed/ controlled by a third party: accompanied to the bank, third party speaks for them or controls documents/money, or the customer gives scripted/inconsistent explanations for transfers. ▶ Multiple accounts (or new accounts) appear opened/used for the same person with no clear purpose, especially where transactions are spread across branches/locations inconsistent with the customer's normal profile.	Trafficking in relation to forced labour (victim)

Inconsistent 'business' activities	▶ Lack of business-related expenses and transactions in corporate bank statements. ▶ The use of personal cheques or accounts in patterns similar to the payment of wages. ▶ Discrepancies between the employees' insurance costs, wages or other related activities in the context of the size of the business. ▶ Higher than average withdrawals or deposits of cash. ▶ Ongoing fines to labour agencies or any current or previous law enforcement investigation into a suspicious transaction. ▶ Unpaid pay-related taxes. ▶ Payments for varying amounts that align with minimum-wage work in the jurisdiction in question. ▶ Payments being deposited back into the account of an employer by the suspected victim. ▶ Payroll deposits for large numbers of employees that are withdrawn in full immediately after transfer. ▶ Business accounts linked to recruitment agencies with high employee turnover and little record of legitimate work contracts. ▶ Payments routed through intermediaries instead of being made directly to employees, suggesting wage withholding or forced labour.	Trafficking in relation to forced labour (perpetrator)
Suspicious transaction activities	▶ Frequent and/or large transactions (e.g. deposits, payments, and transfers) across different cities or provinces within short time frames. ▶ Frequent low value transfers often associated with a subscription or access to content in cyber-lockers. ▶ Multiple incoming deposits or email money transfers from unrelated third parties, often using temporary addresses (e.g. hotels), with little or no explanation.	Trafficking for the purpose of sexual exploitation OCSE (perpetrator)

	▶ Payments to multiple online merchants or classified sites that specialise in digital escort, massage and adult entertainment advertisements. ▶ Purchases that are inconsistent with the customer's profile, including clothing, make-up, beauty products and services, and lingerie. ▶ High volumes of payments to ride-share companies.	
Cross-border and high-risk transfers	▶ Large and frequent electronic transfers between senders and receivers with no apparent personal or business relationship. ▶ Different individuals using a common address when conducting domestic or international funds transfers. ▶ Transactions involving jurisdictions known for high levels of TIP, particularly those with weak AML/Countering the financing of terrorism (CFT) controls.	Trafficking for the purpose of sexual exploitation
Suspicious use of prepaid cards, gift cards, credits to gaming platforms	▶ Prepaid debit and gift cards provide traffickers with an alternative form of payment that is harder to trace. These cards can be used for direct payments or quickly converted into cash or other assets, complicating financial investigations.	OCSE

Financial red flag indicators linked to trafficking in persons: Money value transfer services and virtual assets

Transfer mechanism	Indicators	Link/associated with TIP
VAs including cryptocurrency and DeFi systems These VAs enable users to conduct financial transactions, including lending and borrowing, with increased anonymity (e.g. without stringent KYC protocols) and without government/ authority oversight, making them attractive vehicles for ML	▶ Certain transfers between wallets lacking proper identification or verification can indicate attempts to obscure the origin and destination of funds. ▶ Anonymity-enhancing technologies—criminals leverage services such as mixers and tumblers to obfuscate the origin and flow of illicit funds. By blending tainted cryptocurrencies with clean ones, these services complicate the tracing efforts of LEAs. ▶ Employing privacy coins or decentralised exchanges that do not require KYC procedures. ▶ Quick transfers through multiple virtual asset accounts, especially across different platforms or jurisdictions, may suggest layering to disguise the transaction trail. ▶ Funds deposited into a virtual asset account and promptly withdrawn, particularly in a different form or to another platform, can be a sign of laundering. ▶ Engaging in transactions where the IP addresses are associated with regions lacking robust AML regulations or are known for TIP activities.	OCSE
Peer-to-Peer (P2P) Platforms	▶ For example, mobile money transfer systems (not a digital representation of fiat currency), digital wallets (e.g. PayPal)	OCSE
Unregulated, informal MVTS (e.g. hawala, hundi)	▶ Use of underground banking/ informal value-transfer networks, frequent cross-border transfers via non-bank channels, structured small-value payments, use of cryptocurrency or VASPs, funds flowing from or to known scam-compound jurisdictions, victims instructed to send/receive funds via money-brokers or informal agents, mule accounts and unlicensed brokers handling transfers.	Trafficking for the purpose of forced criminality (victim)

3.3.2 Analysing financial information to develop financial intelligence

Once financial data is collected, thorough analysis is crucial to identify patterns indicative of TIP activities. Steps include:

Data aggregation: Consolidate information from STRs, CTRs and other intelligence sources to create a comprehensive dataset.

Pattern recognition: Employ analytical tools to detect anomalies such as:

- Structuring transactions to evade reporting thresholds.
- Rapid movement of funds through multiple accounts.
- Frequent transactions just below regulatory reporting limits.

Geographical Analysis: FIUs and investigators can potentially map transaction locations to identify hotspots associated with TIP activities.

3.3.3 Mapping networks using financial data and asset tracing

Understanding the network of individuals and entities involved is vital. This involves:

- **Link Analysis:** Connecting individuals, accounts and transactions to reveal relationships within the network.

- **Asset Tracing:** Identifying and tracking assets purchased with illicit funds, such as real estate, vehicles and luxury goods.

- **Beneficial Ownership Identification:** Determining the true owners of accounts and assets, especially when shell companies, nominee arrangements or trusts are used to obscure identities.

Advanced analytical tools can assist in visualising these networks, making it easier to identify key players and their roles.

3.3.4 Identifying, tracing, seizing, freezing and confiscating illicit proceeds

Criminals engage in illegal activity to make a profit. The underlying concept of a ‘follow-the-money’ approach to TIP investigations is to take the profit out of crime by depriving criminals of their illegally gained wealth.

Much like the importance of commencing financial investigations parallel to TIP investigations, an effective approach also simultaneously considers mechanisms to temporarily and permanently deprive criminals of their assets.

- **Identifying assets:** Initiate asset identification early and in parallel with trafficking in persons investigations, focusing on locating direct and indirect proceeds of crime including assets held by third parties through lawful financial analysis, record checks, and cooperation with relevant authorities to support timely provisional measures and eventual confiscation.

- **Provisional measures:** Seek seizing/freezing orders to prevent the dissipation of assets during investigations.

- **Asset forfeiture:** Pursue the legal processes to permanently confiscate proceeds of crime or property of corresponding value to the benefits derived from criminal activity, which can then be repurposed to support victim assistance or crime prevention programmes.

CASE STUDY - Financial Crime Arising From Organ Trafficking

Trafficking in persons for the purpose of organ removal has emerged as a significant form of exploitation, driven by the gap between demand for and supply of transplantable organs. Traffickers targeted economically vulnerable individuals and recruited them under false promises of financial compensation. In the cases identified, donors received only small sums (approximately £360–£610 or USD $660–1,100), while recipients were charged up to INR 200,000 (approximately £2,420) for a kidney.

The District Crime Branch of the Police Department registered criminal cases against 11 doctors for illegally conducting kidney transplants by forging donor identities and fabricating documentation. Under India's Human Organ Transplantation Act, 1994, organ donation is permitted only from immediate family members unless approved by a state authorisation committee, which must verify that donations are not financially motivated. In this case, documents were fabricated to falsely present donors as close relatives or emotionally connected individuals.

Evidence gathered during the trafficking investigation, including forged documentation and statements from donors and recipients, indicated that the illegal transplant operations generated significant financial benefit and involved multiple facilitators, including brokers and medical professionals. These findings were referred to India's Enforcement Directorate (ED), which initiated a parallel financial investigation.

The ED identified a structured network of brokers who recruited prospective donors, collected their medical details, and negotiated fees with recipient patients. The investigation further revealed that illegal payments were made to medical professionals in exchange for endorsing fabricated documentation and approving transplant procedures, despite knowledge that the documents were false. Through financial analysis, the ED identified immovable properties held by the accused that were disproportionate to their legitimate income. These assets, valued at approximately USD $327,300, were provisionally attached. A prosecution complaint was subsequently filed.

This case illustrates how integrating financial investigations into trafficking cases can expose broader organised networks, identify corrupt facilitators, and enable the confiscation of criminal proceeds beyond the immediate trafficking offence.[41][42]

3.4 Technology and advanced analytical tools for financial investigations in trafficking in persons cases

The rapid evolution of financial crime necessitates the use of cutting-edge technology and advanced analytical tools to combat trafficking in persons. Traditional investigative techniques are no longer sufficient, as traffickers and smugglers have adapted to digital payment systems, cryptocurrencies, and sophisticated money-laundering methods. As a result, LEAs, FIUs, and financial institutions have turned to AI, big data analytics, blockchain forensics, and Regulatory Technology (RegTech) solutions to enhance detection, monitoring, and prevention of illicit financial activities.

To stay ahead of evolving TIP typologies, FIUs should explore the integration of advanced analytical tools and technology-driven solutions into their investigative processes. Trend analysis and stakeholder engagement with financial institutions and VASPs help identify emerging patterns in illicit financial flows. The application of AI and data analytics further enhances FIUs' ability to detect suspicious activities by processing vast amounts of transaction data and correlating disparate data points. The International Monetary Fund (IMF) underscores that access to comprehensive financial, administrative, and law enforcement information is essential for FIUs to conduct effective analyses.[43]

41 For more information, see Palaniappan, V.S. (2014) 'ED attaches assets of doctor involved in kidney racket in Chennai', The Hindu, 20 August. Available at: ED attaches assets of doctor involved in kidney racket in Chennai - The Hindu

42 For an additional case study with similar indicators, see Annex 3.

43 International Monetary Fund (2004) *Financial Intelligence Units: An Overview.* Available at: https://www.imf.org/external/pubs/ft/fiu/index.htm

3.4.1 Artificial intelligence and big data analytics in financial investigations

AI has revolutionised financial crime detection by processing vast amounts of financial data to uncover suspicious activity. AI-driven tools are now capable of identifying transaction anomalies, predicting high-risk accounts, and analysing unstructured financial data to recognise hidden connections in complex money-laundering networks. Machine-learning models are used to assess risk profiles by evaluating transaction history, customer behaviour, and regional financial trends. Silent Eight,[44] a leading AI-based compliance platform, enhances AML investigations by automating STR analysis and identifying layering and structuring techniques used in TIP transactions.

Beyond AI, predictive modelling is employed to assess financial risk. It enables investigators to detect high-risk accounts that exhibit patterns consistent with TIP and people-smuggling operations. Tools such as Palantir's Gotham[45] integrate financial transactions, phone records, and digital surveillance data to provide investigators with a comprehensive picture of illicit networks. AI-powered analytics also help identify unusual cross-border transfers, allowing financial institutions to act before funds are laundered through complex networks.

3.4.2 Blockchain forensics for virtual asset tracking

With traffickers increasingly turning to VAs to obscure financial trails, blockchain forensics has become indispensable for financial investigations. Blockchain analysis platforms such as Chainalysis[46] and Elliptic[47] help investigators trace illicit cryptocurrency transactions, de-anonymise crypto wallets, and map out fund flows across multiple jurisdictions. These tools have been instrumental in linking crypto wallets to criminal enterprises, identifying laundering attempts through mixing services and privacy coins, and detecting traffickers who exploit DeFi platforms. INTERPOL has also developed Guidelines on Seizing Virtual Assets,[48] which outline best practices for identifying service providers, maintaining evidence integrity, and adhering to local laws in TIP financial crime cases.

44 Silent Eight. Available at: Iris 7 | Policy-Bound Agentic AI for Financial Crime Compliance
45 Gotham. Available at: Gotham | Palantir
46 Chainalysis. Available at: The Blockchain Data Platform - Chainalysis
47 Elliptic. Available at: Blockchain Analytics & Crypto Compliance Solutions | Elliptic
48 INTERPOL (2023) *Global Guidelines for Seizing Virtual Assets.* Available at: https://www.interpol.int/Crimes/Cybercrime/Projects/C3DP-Cyber-Capabilities-Capacity-Development-Project

3.4.3 Real-time financial transaction monitoring and RegTech solutions

The financial industry has increasingly turned to RegTech solutions to strengthen AML compliance and real-time transaction monitoring. RegTech solutions, such as Actimize AML Suite[49] and Quantexa,[50] use AI to detect abnormal cross-border transfers, structured transactions, and money-laundering schemes linked to TIP/people smuggling. These systems scan transactions against updated regulatory requirements, ensuring that illicit activities are flagged in real time. Platforms such as ComplyAdvantage[51] provide risk intelligence on financial crime networks, helping financial institutions quickly detect and report suspicious activity.

3.4.4 Digital forensic tools for financial investigators

Financial investigators frequently rely on digital forensic tools to extract financial evidence from devices used by traffickers and smugglers. Platforms such as Magnet AXIOM[52] specialise in recovering deleted messages, emails, and financial transaction logs from mobile phones, cloud accounts and encrypted messaging apps such as WhatsApp and Telegram. These tools help investigators map out money mule networks, where traffickers use intermediaries to launder profits from forced labour and sexual exploitation.

---

49 Actimize AML Suite. Available at: NICE Actimize AML Software Solutions
50 Quantexa. Available at: Quantexa - Context Behind Every Decision
51 ComplyAdvantage. Available at: https://complyadvantage.com/
52 Magnet Axiom by Magnet Forensics. Available at: https://www.magnetforensics.com/products/magnet-axiom/

SECTION 4

STAKEHOLDER ENGAGEMENT

A holistic response to trafficking in persons requires collaboration among diverse stakeholders, including multilateral organisations, the private sector, and civil society. Each plays a unique role in assisting competent authorities to implement 'follow-the- money' approaches to TIP.

4.1 Collaboration with the private sector

The private sector, including financial institutions—such as banks, fintech companies and fintech associations, cryptocurrency companies and fast-money-transfer companies—play pivotal roles in the entire life-cycle of a 'follow the money' approach to TIP. This includes:

- Engagement with policymakers to ensure fit-for-purpose legal/regulatory frameworks.
- Compliance with AML obligations (e.g. STR filing, CDD requirements).
- Information sharing and assisting FIUs/LEAs in investigations.

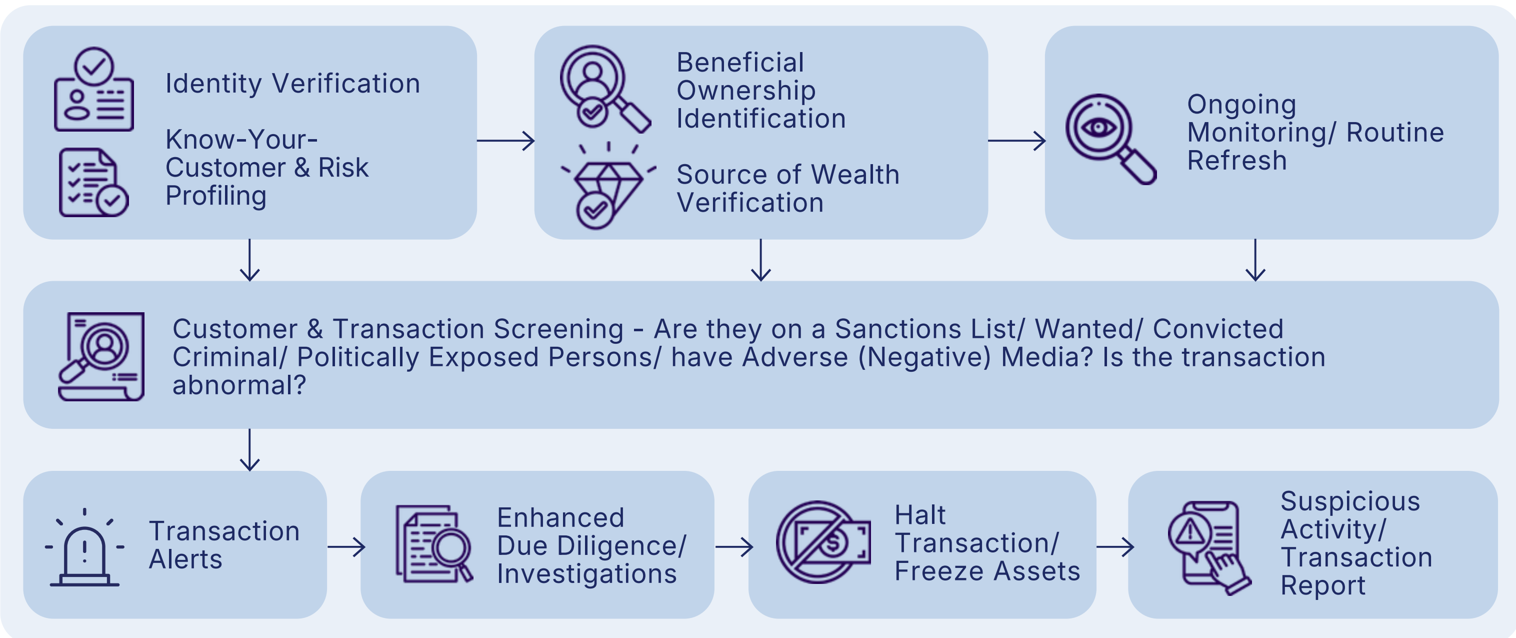


Figure 5. Overview of the customer due diligence and transaction monitoring process. Through these processes, regulated entities such as banks meet their AML compliance obligations and generate the financial intelligence, including suspicious transaction reports, on which 'follow-the-money' investigations and private sector collaboration depend.

The private sector has notably demonstrated a shift towards enhanced technological integration and automation in AML compliance, particularly through the use of AI and machine-learning solutions. Financial institutions have been increasingly channelling resources towards technology that can better detect and report various forms of financial crime, specifically in functional areas such as transaction monitoring, name screening, and customer monitoring. This transformation is especially driven by both regulatory expectations and the imperative to respond more effectively to sophisticated criminal methodologies.[53]

While many reporting entities have made substantial progress in technological adoption and automated detection capabilities, the efficacy of these systems is also enhanced through strengthened public-private partnerships and coordinated intelligence-sharing mechanisms. Automated systems, particularly in areas such as network analytics and customer monitoring, provide a strong foundation for identifying suspicious patterns; however, these capabilities should be complemented by effective channels for sharing actionable intelligence with LEAs. Banks and other financial service providers often collaborate with law enforcement by sharing data patterns, developing red flag indicators, and participating in information-sharing forums.

The FATF has consistently emphasised the importance of public-private sector collaboration in identifying illicit financial flows associated with TIP, ensuring both the public and private sector are identifying and responding to risk proportionately. Encouraging active engagement between FIUs and reporting entities helps refine risk indicators and improve the overall responsiveness of financial systems to emerging threats.

For example, the cyber-scam phenomenon may present a new opportunity for engagement as financial institutions more often need to compensate scam victims for financial losses incurred, meaning it is in their own best interest to improve suspicious transaction flagging and monitoring.

Competent authorities should provide useful feedback to financial institutions on the quality and utility of STRs to enhance the effectiveness of reporting and improve the detection of illicit transactions. Additionally, developing typologies of TIP-related financial activities allows regulated entities to refine their monitoring systems in line with risk and strengthen internal compliance frameworks. Competent authorities (especially supervisors) also play a role in educating relevant sectors about money-laundering risks, vulnerabilities and typologies.

Financial institutions are important partners in identifying suspicious activities related to trafficking. It is recommended to reach out to financial institutions early and regularly to support investigations.

[53] Regulation Asia and NICE Actimize (2024) *AML Tech Barometer 2024 — Rise of the Machine: New Frontiers and Emerging Trends in Detection and Prevention.* Available at: https://info.niceactimize.com/rs/338-EJP-431/images/APAC-AML-Barometer_Report-2024.pdf

CASE STUDY - Public-private partnership example: Australia's Fintel Alliance

Australia's Fintel Alliance is a world-first public-private partnership, demonstrating effective collaboration in combating financial crimes, including those connected to TIP.

Fintel Alliance is an Australian Transaction Reports and Analysis Centre (AUSTRAC) initiative established in 2017 to increase financial sector resilience against criminal exploitation. It also supports law enforcement investigations into serious crime and national security matters. As a public-private partnership, Fintel Alliance brings together experts from various organisations involved in efforts to tackle money laundering, terrorism financing and other serious crimes. Fintel Alliance partners include major banks, remittance service providers and gambling operators, as well as law enforcement and security agencies from Australia and overseas. Working together, Fintel Alliance develops shared intelligence and delivers innovative solutions to detect, disrupt and prevent serious crime.

Fintel Alliance has produced several financial crime guides, including:

- Detecting and stopping forced sexual servitude in Australia
- Combating the exploitation of international students as money mules
- Preventing the criminal abuse of digital currencies

Beyond financial institutions, other private sector actors may have data relevant to TIP that can inform investigations. Although some of these industries are known for facilitating or benefiting from TIP, partnerships and engagement with them are often necessary to prevent and investigate TIP. Examples include:

- social media
- airlines and transportation
- telecommunications
- hotels and other tourism-related industries
- construction companies
- fishing companies
- mining companies

Partnership examples

One example is a partnership between the Thai government and Thai Bankers' Association, which created a shared protocol for identifying suspicious financial activities that may indicate TIP. Bank staff were trained to flag and report high-risk transactions, such as high remittances to trafficking hotspots, leading to quicker intervention by authorities.

Another example is in the United States, where the Center for Countering Human Trafficking (CCHT), led by Homeland Security Investigations, established partnerships with banks, money remittance services, and mobile payment apps. These partners share specific Suspicious Activity Reports (SARs) with the CCHT that they have identified as significant or actionable. The CCHT then evaluates leads and refers them to field offices for follow-up.

4.2 Collaboration with multilateral organisations

Given the cross-jurisdictional nature of TIP, multilateral organisations play a central role in helping countries track and disrupt the financial networks fuelling TIP operations. They can contribute by facilitating cooperation and coordination, enabling information and data sharing, and providing capacity building for competent authorities on 'follow-the-money' investigations in TIP cases.

There are various programmes across the region that already provide several types of assistance for governments, including APG, UNODC, IOM, ILO, the Bali Process Regional Support Office and ASEAN-Australia Counter Trafficking (ASEAN-ACT). Consider reaching out to these organisations with specific requests or priority areas.

CASE STUDY - Cross-Border Asset Recovery Collaboration Between the Republic of Indonesia and New Zealand

Background

The Asset Recovery Inter-Agency Network for Asia Pacific (ARIN-AP) is a collaborative group of specialists from multiple states that provides specific support in the confiscation and recovery of illicit assets in the Asia Pacific region. There are 28 Member States in the network, of which 22 are also Bali Process Members. ARIN-AP works to create a hub of regional expertise on criminal asset recovery and shares expertise across the region. Although it focuses efforts on the recovery of assets derived from all serious crimes, ARIN-AP plays a crucial role in recovering assets linked to TIP crimes due to its regional prevalence.

Collaboration through ARIN-AP

In 2023, the Republic of Indonesia's Asset Recovery Body, operating under the Attorney General's Offices, initiated a significant cross-border asset recovery case. As the designated contact point of ARIN-AP in the Republic of Indonesia, the Asset Recovery Body reached out to its counterparts in New Zealand through the Crown Solicitor. After this contact, the Asset Recovery Unit of the New Zealand Police began collecting evidence. This investigation led to the submission of a Non-Conviction-Based Asset Forfeiture application to the Invercargill High Court regarding a property in New Zealand. The efforts of both countries' authorities proved successful, as the property was sold for NZD 5.2 million (USD $3.2 million).

CASE STUDY - ASEAN Convention against TIP (ACTIP)

Background

Southeast Asia's extensive borders and the high mobility of its population are enabling factors for TIP operations. Victims are often recruited across borders with promises of jobs that pay better than those available in their location of origin. After being trafficked to a destination, TIP victims often have their passports confiscated and their movement restricted.

ACTIP was introduced in response to the prevalence of TIP in the region. There has also been a growing awareness that responses to TIP must emphasise victim protection and support.

Solution: collaboration

In order to address shortfalls in the protection of victims, the US partnered with the Association of Southeast Asian Nations (ASEAN) and the ASEAN Commission on the Promotion and Protection of the Rights of Women and Children (ACWC) to strengthen victim protection measures. This initiative seeks to promote the ethical treatment of trafficking victims through stakeholder education and the provision of state support to lower the risk of victims being re-trafficked. This has primarily involved multinational training sessions and curriculum development to empower state actors to train law enforcement personnel. They have also engaged CSOs in collaborative efforts between sectors to combat TIP. This collaboration programme has proved beneficial, with numerous participants from Southeast Asia noting the benefits of such an approach.

Other best practices for protecting TIP victims:

- Ensure the responsible re-allocation of seized criminal assets to victims;
- Ensure the physical safety of victims and provide asylum if their physical safety cannot be guaranteed;
- Provide essential documents for repatriation as necessary;
- Hold origin states accountable for creating safe environments for repatriated victims;
- Support countries to develop policies and procedures on victim return and reintegration.

4.3 Collaboration with civil society organisations

CSOs are essential in understanding, responding to and preventing TIP. This includes data collection and analysis regarding modus operandi and payment methods, organising community outreach and education programmes that help reduce vulnerabilities, offering economic alternatives and support to vulnerable groups, or raising awareness on risks and vulnerabilities to trafficking. CSOs often also support and rescue TIP victims, in addition to assisting with reintegration.

As such, CSOs are key partners in understanding and combating TIP. Competent authorities can leverage this local expertise and data to reduce administrative burdens in understanding TIP in a particular jurisdiction. Additionally, countries should seek to engage CSOs regularly to ensure an up-to-date understanding of TIP trends and typologies.

With the rise of online recruitment and digital payments, collaboration with tech companies and CSOs specialising in digital rights has become critical. Authorities should work with both sectors to track cryptocurrency transactions and mobile payments, which are increasingly used by traffickers. For example, CSOs can contribute their expertise in digital privacy laws and human rights considerations, whereas tech companies can assist in tracing encrypted financial transactions and uncover wider transnational criminal organisations.

CSOs can also create and implement training programmes for both the public and private sector. These can focus on the nexus between TIP and money laundering, covering topics such as red flag recognition, effective collaboration, and information sharing to quickly respond to suspected trafficking-related financial crimes.

Some private sector companies have partnered with authorities to help compensate TIP victims by contributing a portion of recovered or forfeited assets. This initiative has ensured that victims receive financial support to rebuild their lives, often facilitated through CSOs who manage the distribution of these funds. In addition, partnerships with CSOs are crucial to provide legal assistance for victims to obtain compensation.

Partnership examples

- Australia hosts an annual ministerial National Roundtable on Human Trafficking and Slavery as a consultative mechanism between the Government, NGOs and other partners on human trafficking and wider modern slavery policy, legislation and reform. The National Roundtable is supported by a senior officials' meeting, which also comprises government and non-government representatives.

- In cooperation with the International Justice Mission (IJM), Thailand has developed frameworks enabling this collaboration. CSOs can help investigators by providing background on victim recruitment, salary siphoning and traffickers' financial mechanisms. This information supports the 'follow-the-money' approach by tracing money flows that reveal broader trafficking networks.

- The Global Initiative against Transnational Organized Crime (GI-TOC)'s Resilience Fund[54] supports organisations responding to TIP in Asia, Latin America and Africa. This support has involved training stakeholders and partners on understanding and responding to TIP, including the use of technology in TIP. For instance, the Resilience Fund has enabled First Step Cambodia to conduct advocacy work on digital sexual exploitation in Cambodia.

- Through collaboration with the Anti-Human Trafficking Fund in Thailand, several private companies pool resources for direct financial support to victims identified during trafficking investigations. This multi-stakeholder approach creates a holistic recovery system.

- Information exchange platforms are another important response to TIP. For example, the Global Missing Children's Network, supported by the International Centre for Missing and Exploited Children (ICMEC), brings together institutions, regulators, LEAs and civil society. The organisation maintains a digital platform that compiles information related to missing and abducted children and supplies information to the relevant authorities to help with investigations.

[54] The Global Initiative against Transnational Organized Crime's Resilience Fund complements and builds on the Global Initiative's ongoing work in incubating resilience in communities harmed or threatened by criminal governance. Available at: https://globalinitiative.net/initiatives/resiliencefund/

SECTION 5

INTERNATIONAL COOPERATION

Given the inherently transnational nature of TIP, as well as the associated financial flows, regular and timely international cooperation is critical to a successful TIP investigation.

5.1 Financial intelligence unit-to-financial intelligence unit networks

FIUs play a pivotal role in detecting and combating financial crimes associated with TIP by exchanging financial intelligence from STRs, CTRs, and other reports with their counterparts globally. Collaboration between FIUs across jurisdictions enhances the effectiveness of financial investigations and analysis and is required under Recommendation 40 of the FATF Standards.

Establishing structured information-sharing mechanisms and leveraging secure communication platforms can enhance coordination across jurisdictions. However, challenges such as procedural delays, language barriers, and limitations on using shared financial intelligence as legal evidence continue to hinder seamless collaboration. Strengthening bilateral and multilateral agreements on financial intelligence sharing is crucial for overcoming these barriers and ensuring the effective use of intelligence in multi-jurisdictional cases.

Egmont Group: A global network that promotes secure information sharing and collaboration to combat money laundering and terrorist financing among 167 FIUs worldwide. Through the Egmont Secure Web, member FIUs can exchange information swiftly, aiding in the identification and tracing of illicit financial activities linked to TIP.

5.2 Law enforcement agency-to-law enforcement agency networks

Much like FIUs, effective cooperation between LEAs is crucial to achieving TIP and financial investigation outcomes. In accordance with Recommendations 38 and 40 of the FATF Standards, LEAs should be able to exchange information with foreign counterparts for ML or TIP investigations, and to support the identification, tracing, freezing, seizing and confiscation of assets.

Key networks facilitating this cooperation include:

- **Asset Recovery Inter-Agency Networks (ARINs):** Regional networks that facilitate the exchange of information and best practices among law enforcement and judicial authorities to identify, trace and recover illicit assets. By leveraging ARINs, agencies can enhance their capacity to disrupt the financial infrastructure of trafficking and smuggling networks.

Competent authorities can also leverage INTERPOL mechanisms to advance financial investigations, including:

- **INTERPOL Global Rapid Intervention of Payment (IGRIP):** A real-time system for stopping, recalling and recovering fraudulent transactions linked to TIP and people smuggling, which replaced the older Anti-Money Laundering Rapid Response Protocol (ARRP). It is used by multiple countries to halt illicit payments before they are withdrawn and is supported by INTERPOL's I-24/7 global communication system.

- **INTERPOL Global Register of Illicit Assets (IGRIA):** Assists Member States in identifying and tracing seized/confiscated assets linked to organised crime.

- **INTERPOL Notices[55] (Silver, Purple, Blue, and Red Notices):**
  - Silver Notices: Allow Member States to trace and seize criminal assets, including bank accounts, real estate and virtual assets linked to TIP and people smuggling.
  - Purple Notices: Used to share modi operandi of trafficking and smuggling groups.
  - Blue Notices: Used to locate and track TIP suspects.
  - Red Notices: Used to seek the arrest of traffickers and smugglers for extradition.

5.3 Other types of international cooperation

5.3.1 Mutual Legal Assistance requests and international cooperation frameworks

Formal mechanisms for international cooperation are vital for obtaining evidence and enforcing legal actions across borders. Mutual Legal Assistance Treaties (MLATs) and other frameworks enable countries to collaborate effectively. Key aspects include:

- **MLA Requests:** These are formal requests between governments seeking assistance in gathering evidence or executing legal processes pertinent to criminal investigations and prosecutions. In the context of TIP and people smuggling, MLA requests can facilitate the sharing of financial records, witness testimonies, and other critical information necessary for comprehensive investigations.

- **International Cooperation Frameworks:** Instruments such as the UNTOC and its supplementary protocols provide a foundation for international collaboration. These frameworks obligate signatory states to assist each other in investigations, prosecutions, and judicial proceedings related to transnational crimes.

55 INTERPOL. *INTERPOL Notices*. Available at: https://www.interpol.int/en/How-we-work/Notices

For regional coordination on addressing TIP in Southeast Asia, the Voluntary Lead Shepherd of the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) is responsible for fostering collaboration among ASEAN Member States, facilitating discussions, and guiding the development of policies and action plans aimed at combating TIP. This role involves spearheading collective actions such as enhancing victim protection, strengthening law enforcement cooperation, and improving cross-border coordination.

SECTION 6

KEY TAKEAWAYS AND NEXT STEPS

While significant progress has been achieved since the publication of the initial *Bali Process Policy Guide on Following the Money in Trafficking in Persons Cases*, emerging and persistent challenges necessitate continued adaptation and response.

Four key priorities for the future include:

- **Enhancing information gathering:** TIP operations are increasingly becoming sophisticated and diverse. Understanding emerging trafficking methods, shifting modus operandi and the complex operations of transnational criminal organisations requires improved information gathering and sharing across the entire criminal supply chain. This includes mapping financial flows, identifying new trafficking routes, and documenting evolving recruitment tactics.

- **Improving investigation of enabling environments:** More focus should be put on understanding and investigating enabling environments, key financial facilitators and institutional vulnerabilities. Through understanding how money moves through the system, agencies can better target interventions to disrupt trafficking operations at their most vulnerable points.

- **Implementing holistic, multi-stakeholder approaches:** The counter-trafficking response should expand beyond law enforcement and criminal justice instruments. A holistic response should combine 'following-the-money' approaches with victim-centred approaches, and involve coordination between FIUs, law enforcement, civil society and the private sector to best ensure support for victims while also disrupting criminal networks.

- **Expanding focus beyond formal financial systems:** Response strategies should involve formal financial systems, while also recognising the ways in which transnational criminal organisations utilise informal financial networks. Responses should balance AML regulations in formal sectors with targeted interventions in informal financial systems. Furthermore, addressing TIP-related money-laundering risks in the informal economy will become more important if traditional AML approaches become less effective as the global financial system becomes increasingly complex.

6.1 Key areas of focus

6.1.1 Understanding the risks, threats, vulnerabilities and typologies

The past decade has seen rapid technological developments reshaping TIP in the Bali Process region. Increased use of fintech and cryptocurrencies has created new opportunities and tools with which to exploit victims and launder money. These developments are commonly cited as the most critical challenge among responding agencies.

Technological developments, however, also offer opportunities to enhance the current response. For instance, AI and big data analytics can help with pattern recognition and risk assessment. Stakeholders can use these insights to establish early warning systems and facilitate data sharing.

6.1.2 Conducting financial investigations

- Implement policies that require financial investigations to be conducted parallel to all TIP cases. This ensures systematic collection of financial evidence, increasing the likelihood of identifying and prosecuting financial facilitators. Authorities must integrate financial investigative techniques into routine law enforcement operations to disrupt criminal networks effectively.

- Strengthen the collection, analysis, and utilisation of STRs and CTRs related to these crimes. Develop specialised risk-based indicators to identify suspicious transactions linked to TIP and people smuggling. Ensure that relevant financial intelligence is promptly disseminated to LEAs to enable proactive enforcement action.

- Establish secure real-time communication channels and standardised protocols for financial intelligence exchange between Member States.

- Facilitate direct cooperation between FIUs, LEAs and regulatory bodies to enhance cross-border financial investigations.

- Develop regional databases and intelligence-sharing platforms to detect and track illicit financial flows associated with trafficking and smuggling networks. Provide dedicated training programmes for financial investigators, law enforcement personnel, prosecutors and judiciary members on financial investigative techniques, asset tracing and cross-border cooperation. Capacity-building efforts should focus on increasing expertise in analysing complex financial transactions and dismantling illicit financial networks.

6.1.3 Integration of technological solutions

- Encourage the adoption of advanced financial intelligence tools, blockchain analytics, and artificial-intelligence-driven risk assessment systems to enhance the detection and tracking of illicit financial flows associated with TIP and smuggling.

6.1.4 Asset tracing and confiscation

- Ensure legal frameworks to freeze, seize and confiscate illicit proceeds align with international standards, such as FATF Recommendations, to enhance the effectiveness of asset recovery measures. Ensure also that the legal framework grants clear authority to freeze, seize and confiscate virtual assets.

- Apply proportionate and effective sanctions against individuals and entities involved in these crimes, including travel bans, asset freezes and restrictions on financial transactions. Develop mechanisms for monitoring compliance with these sanctions and ensuring their enforcement at the national and regional levels.

- Adopt non-conviction-based asset forfeiture measures to recover illicit assets when criminal prosecution is not feasible, in accordance with a State's domestic laws and the prevailing FATF Standards. Ensure these measures comply with human rights protections while effectively depriving criminals of their unlawful gains.

- Explore the establishment of specialised units/mechanisms for managing confiscated assets, including ensuring their effective utilisation for victim compensation and reinvestment in counter-trafficking initiatives, in accordance with a State's domestic laws and the prevailing FATF Standards.

6.1.5 International cooperation

Currently, addressing TIP requires enhanced cooperation, capacity building and investment in technology for law enforcement so they can stay ahead of traffickers and their evolving money-moving and laundering tactics. This is a global issue that no country can manage on its own.

- Enhance collaboration through FIUs and international organisations such as INTERPOL and UNODC to share intelligence on cross-border financial activities. Establish joint investigative teams to conduct transnational financial crime investigations.

- Ensure national policies and practices are consistent with FATF Recommendations, relevant United Nations conventions, and regional AML/CFT frameworks. Regularly review and update domestic legislation to maintain compliance with evolving international obligations.

- Strengthen legal frameworks and diplomatic protocols for cross-border asset recovery and extradition of offenders involved in TIP.

6.1.6 Multi-sector engagement

- Collaborate with financial institutions and, where relevant, blockchain analytics providers to develop and disseminate red flag indicators for detecting suspicious transactions linked to trafficking and smuggling networks. Conduct continuous training programmes to enhance the capacity of financial sector personnel in identifying and reporting such transactions.

- Ensure robust AML/CFT compliance within financial institutions. Conduct regular audits, compliance checks, and regulatory inspections to detect vulnerabilities and ensure adherence to financial crime prevention measures.

- Foster partnerships between government agencies, financial institutions, social media companies, and technology service providers to facilitate information sharing and collaborative efforts in detecting and preventing financial crimes. Develop real-time reporting systems and automated monitoring tools to enhance detection capabilities.

- Encourage the use of AI, blockchain analysis, and big data analytics to improve the identification of illicit financial flows and enhance financial intelligence capabilities. Facilitate cross-border adoption of advanced digital tools for transaction monitoring and risk assessment.

- Strengthen regulatory mechanisms for monitoring high-risk financial sectors, such as remittance service providers, VASPs (including exchanges and stablecoin issuers) and informal value transfer systems. Ensure these sectors implement stringent due diligence measures and comply with AML/CFT regulations.

- Launch awareness campaigns to educate financial sector stakeholders, businesses and the general public about the financial dimensions of TIP and people smuggling. Promote ethical financial practices and encourage the reporting of suspicious activities to relevant authorities.

- Promote the inclusion of civil society organisations, academic institutions, and financial industry experts in policy monitoring and evaluation efforts. Their insights will contribute to refining strategies and ensuring a holistic approach to combating illicit financial activities.

6.2 Training and capacity building for financial investigators

Develop and conduct regular capacity-building programmes tailored for AML/CFT investigators, prosecutors, judicial authorities and relevant stakeholders. These programmes should focus on specialised financial investigative techniques, international cooperation mechanisms, asset recovery strategies, typologies, and technological advancements in financial crime detection.

6.2.1 Essential skills for financial investigators

Tracing financial flows across various sectors

- **Banking sector:** Investigators must be adept at analysing bank records to identify suspicious transactions, understand complex financial products, and detect anomalies indicative of money laundering related to TIP.

- **Virtual assets:** With the rise of virtual currencies, proficiency in blockchain analysis is crucial. FIU analysts, prosecutors and regulators should have the training required to identify virtual-asset-related threats. Investigators should have the training to identify virtual-asset-related artefacts such as wallet addresses and seed phrases, and the data and technical tools for rapid initial triage and more in-depth analysis. Specialist expertise, whether in-house or external, may be required in some cases to tackle complex investigations and the use of obfuscation mechanisms.
  - **Cryptocurrency:** With the rise of digital currencies, proficiency in blockchain analysis is crucial. Investigators should be capable of tracing cryptocurrency transactions, recognising the use of mixing services, and understanding the methods traffickers use to exploit digital assets.

- **Informal financial systems:** Knowledge of systems such as hawala is essential, as traffickers often use these networks to move funds outside formal banking channels. Understanding the mechanics of these systems aids in identifying and tracking illicit financial activities.

Analysing financial patterns specific to TIP networks

- **Identifying red flags:** Recognising indicators such as frequent small cash deposits, rapid movement of funds between accounts, and transactions inconsistent with a customer's profile can signal TIP activities.

- **Network analysis:** Utilising data analytics to map relationships between entities and individuals helps uncover the structure of trafficking networks and the flow of illicit funds. For instance, in the case of VAs, identifying consolidation points (intermediary wallets into which financial flows are consolidated before being dispersed again as part of the layering process, or sent to a VASP for off-ramping) can be valuable in helping to analyse broader networks.

- **Sector-specific typologies:** Understanding how different industries, such as hospitality or agriculture, may be exploited for money laundering enables investigators to tailor their analytical approaches accordingly.

Simulation exercises and practical case studies: incorporating real-life scenarios into training

- **Case-based learning:** Engaging with actual case studies allows investigators to apply theoretical knowledge to real-world situations, enhancing their problem-solving abilities. For instance, the International Association of Chiefs of Police (IACP) offers online self-paced training that includes TIP case examples and statutes, providing practical insights into financial crimes associated with trafficking.[56]

[56] International Association of Chiefs of Police (2025) *Financial Crime and Human Trafficking.* Available at: https://learn.theiacp.org/products/financial-crime-and-human-trafficking

- **Interactive Simulations:** Participating in simulations that mimic real-world financial crime scenarios enables investigators to practice tracing illicit funds, making decisions under pressure, and collaborating with other agencies. The Basel Institute on Governance provides training programmes that use extensive hands-on practical exercises, including country-specific simulated investigations, to enhance participants' skills in financial investigations and asset recovery.[57]

Providing interactive tools and case study repositories for hands-on learning

- **Digital platforms:** Utilising online platforms that offer interactive tools, such as transaction monitoring systems and data visualisation software, helps investigators practice and refine their analytical skills.

- **Access to case repositories:** Maintaining a database of anonymised case studies allows investigators to study various typologies of financial crimes related to TIP, learning from past investigations to inform future efforts.

- **Continuous learning opportunities:** Encouraging participation in webinars, workshops and conferences keeps investigators updated on emerging trends and techniques in financial crime investigation. Organisations such as the Association of Certified Anti-Money Laundering Specialists (ACAMS) offer webinars that share real-life case studies exploring how FIUs identify complex money-laundering scenarios. Jurisdictions are also encouraged to promote their own analytical products, typology reports and case-based studies to support practitioner learning. For example, the 2023 interim report Understanding OSAEC Trafficking in the Philippines describes clear red flags, payment behaviours, and financial patterns relevant to technology-facilitated exploitation.[58] Similar case studies can strengthen regional understanding and enhance collective investigative skills.

---

57 Basel Institute on Governance (2017) *Training Programmes: Financial Investigations and Asset Recovery*. Available at: https://baselgovernance.org/sites/default/files/2019-02/ICAR_Training_Programmes_2017.pdf

58 Justice and Care (2023) *Understanding OSAEC Trafficking in the Philippines*. Available at: https://justiceandcare.org/app/uploads/2023/11/Understanding-OSEAC-Trafficking-in-the-Philippines-Interim-Report_October-2023.pdf

ANNEX 1

GLOSSARY

Term	Definition
Anti-money laundering (AML)	A set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. AML regulations require financial institutions to monitor customers' transactions and report suspicious activities to relevant authorities.
Artificial intelligence (AI)	Technology that allows computer systems to learn from data and perform tasks such as recognising patterns, making predictions or decisions, and generating content in ways that resemble some aspects of human intelligence
ASEAN Convention against Trafficking in Persons (ACTIP)	A regional treaty adopted by the ASEAN in 2015 that aims to prevent and combat trafficking in persons, protect and assist victims, and promote cooperation among ASEAN Member States in the fight against TIP.
Beneficial owner	The natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Blockchain analytics	The process of examining, identifying, clustering, modelling and visually representing data on a blockchain to identify trends, patterns and other information. It is used in financial investigations to trace the movement of virtual assets and identify transactions linked to criminal activity.
Cryptocurrency	A type of virtual asset (see below), i.e. any form of currency that only exists digitally and usually has no central issuing or regulating authority but instead uses a decentralised system to record transactions and manage the issuance of new units.
Fiat currency	Government-issued legal tender that is not digital-only and is regulated by central banks.

Term	Definition
Fiat rails	Fiat rails refer to the regulated banking and payment infrastructures that enable the movement of government-issued currency through formal channels such as bank transfers, real-time payment systems, and card networks. Within the Bali Process region, examples include Thailand's PromptPay system, which enables instant low-cost transfers using national ID or phone numbers, India's Unified Payments Interface (UPI), and Singapore's FAST/PayNow network for near-real-time domestic payments. These rails are central to everyday economic activity, while also shaping how financial flows can be monitored, traced, or misused depending on the strength of regulatory and supervisory controls.
Financial Action Task Force (FATF)	An intergovernmental organisation founded in 1989 to develop policies to combat money laundering, terrorist financing (since 2001) and proliferation financing (since 2008). FATF sets global standards and promotes effective implementation of legal, regulatory and operational measures for fighting money laundering, terrorist financing and other related threats to the integrity of the international financial system.
Financial Intelligence Unit (FIU)	Defined under FATF Recommendation 29, a Financial Intelligence Unit is a national centre for the receipt and analysis of STRs and other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.
Financial Technology (FinTech)	New technology that seeks to improve and automate the delivery and use of financial services.
Hawala and hundi systems	Informal remittance systems that operate outside traditional banking channels and utilise a network of money brokers ('hawaladars').
Illicit financial flows	Illegal movements of capital across international borders.
Illicit proceeds	Funds or assets derived from criminal activity. These proceeds are often the target of money-laundering schemes, where criminals attempt to disguise the origin of the funds to make them appear legitimate.

Term	Definition
Money laundering (ML)	The act by which the proceeds of crime are made to appear legitimate.
Money or Value Transfer Services (MVTS)	Financial services that involve the acceptance of cash, cheques or other monetary instruction or stores of value, and the payment of a corresponding sum in cash or other form to a beneficiary, by means of a communication, message, transfer, or through a clearing network to which the MVTS belongs.
Proceeds (and instruments) of crime	Proceeds of crime refers to any property derived from or obtained, directly or indirectly, through the commission of a criminal offence. Instruments are property that is used in or in connection with predicate crimes or ML.
Regulators/supervisors	FATF-identified regulators are the governmental or regulatory bodies within a jurisdiction that are responsible for setting and enforcing anti-money laundering (AML) and counter-terrorism financing (CTF) rules. Supervisors are the specific individuals or entities within these regulatory bodies who are tasked with overseeing how financial institutions and designated non-financial businesses and professions (DNFBPs) implement AML/CTF obligations.
Regulatory Technology (RegTech)	Technology that assists businesses in meeting regulatory requirements efficiently and cost-effectively. In the context of AML/CFT, RegTech includes solutions for transaction monitoring, customer due diligence, sanction screening and regulatory reporting.
Risk-based approach (RBA)	An approach to identify, assess and understand the ML risk to which jurisdictions are exposed, and take the appropriate and proportionate mitigation measures in accordance with the level of risk. This includes taking enhanced measures where risks are higher and taking simplified or lesser measures where risks are lower.

Term	Definition
Special economic zones (SEZs)	An area in a country that is designed to generate positive economic growth and is normally subject to different and more favourable economic regulations compared to other regions in the same country, including tax incentives and the opportunity to pay lower tariffs.
Stablecoins	A type of cryptocurrency designed to minimise price volatility by being pegged to a stable asset like fiat currency, precious metals or a basket of goods. Stablecoins aim to combine the instant processing, security and privacy of cryptocurrencies with the stable value of traditional currencies.
Trade-based money laundering (TBML)	The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.
Trafficking in persons (TIP)	The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability, or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.
United Nations Convention Against Transnational Organized Crime (UNTOC)	Also known as the Palermo Convention, this is the main international instrument in the fight against transnational organised crime. Adopted in 2000, it obligates Member States to implement measures against transnational organised crime, including money laundering, corruption and obstruction of justice, while promoting international cooperation.
Virtual assets (VAs) and Virtual Asset Service Providers (VASPs)	Digital representations of value that can be digitally traded or transferred, and can be used for payment or investment purposes, but do not include digital representations of fiat currencies, securities and other financial assets. This broader term includes cryptocurrencies and other digital tokens.

ANNEX 2

HOW DOES TRAFFICKING IN PERSONS RELATE TO PEOPLE SMUGGLING?

UNTOC defines TIP as the recruitment, transportation, transfer, harbouring or receipt of persons through threat, force, or coercion for the purpose of exploitation.[59] In contrast, the Protocol against the Smuggling of Migrants by Land, Sea and Air defines people smuggling as facilitating the illegal entry of a person into a State Party of which the person is not a national or a personal resident.[60] In short, while irregular migration and TIP often share similar drivers—including conflict and political instability, economic hardship, corruption and gender inequalities—they are distinct offences. TIP involves exploitation, whereas smuggling primarily concerns illegal border crossing.

Nevertheless, significant conceptual confusion between TIP and people smuggling persists across the Bali Process region. This misunderstanding can be observed in national policies and policing, and even the work of non-state actors supporting migrant rights. The resulting conflation of these issues as general 'trafficking' or 'migration crime' hampers effective responses to each distinct problem.

There are several reasons for the prevalence of TIP in the Bali Process region, making it a challenging crime to address. Economic vulnerability combined with high regional mobility creates a context in which many people seek employment and opportunities across borders. Due to barriers to movement and regular migration, some people use smugglers to move throughout the region. These irregular migrants often take work in the informal sector, which increases the risk of exploitation. UNODC has estimated that smugglers facilitate the substantial majority of irregular migration in Southeast Asia, with earlier analysis placing the figure at approximately 80 per cent.[61]

Intercepting irregular migrants and addressing root causes, including targeting criminal facilitators, are equally essential and mutually reinforcing. Strategies that prioritize one element in isolation risk limiting overall effectiveness in reducing irregular migration and protecting individuals in vulnerable situations. A more holistic approach that targets traffickers, enhances protections for migrants, and addresses labour market demands could help reduce irregular migration while protecting vulnerable individuals and improving border management.

59 United Nations (2000) *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime.* Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons

60 United Nations (2000) *Protocol against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention against Transnational Organized Crime.* Available at: https://www.unodc.org/documents/middleeastandnorthafrica/smuggling-migrants/SoM_Protocol_English.pdf

61 United Nations Office on Drugs and Crime (2017) *Enhancing Law Enforcement Responses to Migrant Smuggling in Thailand.* Available at: https://www.unodc.org/roseap/en/2017/05/migrant-smuggling-thailand/story.html

Moving ahead, it is crucial to distinguish between people smuggling and TIP. Efforts should focus on building knowledge of both phenomena, enabling the development of appropriate responses and 'follow-the-money' investigation strategies. Additionally, understanding the broader ecosystem in which both crimes occur, including their potential links to other forms of organised crime, is essential for crafting impactful solutions.

ANNEX 3

CASE STUDY - FINANCIAL CRIME ARISING FROM TRAFFICKING IN RELATION TO FORCED LABOUR

Following the rescue of nine victims of trafficking in persons, a charge sheet was filed by the agency investigating the predicate trafficking offence. Based on this referral, India's Enforcement Directorate (ED), under the Ministry of Finance, initiated a parallel financial investigation.

The investigation identified that the accused and their accomplices operated placement agencies that recruited vulnerable girls for domestic work. Wages paid by employers were collected directly by the placement agencies, while victims received no remuneration, despite having worked for extended periods. The accused also received commissions from employers for each placement.

The placement agencies were operating without the required licence under the Delhi Private Placement Agencies (Regulation) Order, 2014, and none of the trafficking victims were registered under the Inter-State Migrant Workmen (Regulation of Employment and Conditions of Service) Act, 1979.[62]

Financial analysis indicated that the network had generated proceeds exceeding INR 50 million (approximately USD 550,752) through the placement of an estimated 5,000–6,000 boys and girls in domestic work and other forms of employment. The ED identified and attached substantial assets worth USD 370,105 held by the accused that were disproportionate to their declared income.

Victim statements were recorded, unexplained assets were provisionally attached, and the ED filed a prosecution complaint against the accused and their accomplices under India's anti-money laundering legislation, the Prevention of Money Laundering Act.[63]

[62] The Inter-State Migrant Workmen (Regulation of Employment and Conditions of Service) Act, 1979, protects workers recruited from one state for employment in another by mandating registration of establishments and licensing of contractors for those employing 5 or more inter-state migrant workmen. It ensures equal pay, displacement allowances (50% of wages), journey allowances, suitable housing, and medical facilities. Available at: https://clc.gov.in/clc/acts-rules/interstate-migrant-workmen-act#:~:text=The%20Act%20is%20intended%20to,Central%20and%20State%20Sphere%20respectively.

[63] For more information, see Pandey, M.C. (2022) *India Today*. 'ED attaches assets worth Rs 3.36 crore of human trafficking kingpin'. Available at: ED attaches assets worth Rs 3.36 crore of human trafficking kingpin - India Today

ANNEX 4

FURTHER RESOURCES

Resource	Short description	Frequency
Trafficking in Persons (TIP) Report (USA)	The United States' TIP Report is the U.S. Government's annual assessment of government efforts to combat trafficking in persons. It includes country tier rankings and country narratives outlining progress made and remaining gaps.	Annual
Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings Report	This annual report outlines the office's activities, priorities, and engagement on combating trafficking in human beings during the reporting period.	Annual
Global Report on Trafficking in Persons	The Global Report on Trafficking in Persons is released by UNODC and provides a snapshot of trafficking patterns and flows around the world.	Every two years
World Migration Report	The World Migration Report, published by IOM, looks at changes occurring in migration and mobility globally. It also addresses the nexus with trafficking in persons and migrant smuggling.	Every two years
Global Organized Crime Index	The GI-TOC Global Organized Crime Index provides insights into criminal markets, criminal actors, and state resilience at the national level, including trends relevant to trafficking in persons and migrant smuggling.	Every two years
Following the Money 2.0: A Collaborative Approach to Human Trafficking Investigations Involving Virtual Assets	This OSCE guide supports financial investigations in trafficking in persons cases, with a particular focus on virtual assets, cross-border financial trails, and collaborative investigative approaches.	No fixed schedule

Resource	Short description	Frequency
The Business of Exploitation: The Economics of Cyber-Scam Operations in Southeast Asia	This GI-TOC report examines the financial architecture of cyber-scam operations in Southeast Asia, including payment systems, laundering mechanisms, worker exploitation and trafficking for forced criminality, and corruption payments. It also provides policy recommendations for disrupting the profitability of these operations.	No fixed schedule
Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia	This UNODC report examines the expansion of scam centres, underground banking, and illicit online marketplaces in Southeast Asia, and their implications for transnational organised crime and trafficking-linked exploitation.	No fixed schedule
Detecting, Disrupting and Investigating Online Child Sexual Exploitation	This FATF report provides analysis on financial flows, typologies, and investigative approaches related to online child sexual exploitation, making it a useful complementary resource on exploitation and financial crime.	No fixed schedule
International Co-operation on Money Laundering Detection, Investigation and Prosecution Handbook	This jointly produced handbook by FATF, the Egmont Group, INTERPOL and UNODC promotes stronger international cooperation in money laundering detection, investigation, and prosecution, including through informal cooperation and information-sharing mechanisms.	No fixed schedule
Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia	This UNODC technical policy brief examines casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. It also provides recommendations to improve knowledge, awareness, policy, capacity, and coordination.	No fixed schedule
Counter Trafficking Data Collaborative	The Counter Trafficking Data Collaborative makes counter-trafficking data available to support analysis of victims, cases, and trafficking trends.	No fixed schedule

Resource	Short description	Frequency
Migration Data Portal	The Migration Data Portal provides an access point to migration data and statistics, including a dedicated theme page on human trafficking.	No fixed schedule

The Bali **Process**