Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings

FOLLOWING THE MONEY 2.0

A Collaborative Approach to Human Trafficking Investigations Involving Virtual Assets

OSCE Organization for Security and Co-operation in Europe

ISBN: 978-92-9271-554-0

Published by the OSCE Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings and OSCE Department of Management and Finance

Wallnerstr. 6, 1010 Vienna, Austria
Tel: + 43 1 51436 6664
Fax: + 43 1 51436 6299
email: info-cthb@osce.org

Design: Tina Feiertag, Vienna
Illustrations: shutterstock

Cite as: OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings
Following the Money 2.0: A Collaborative Approach to Human Trafficking Investigations Involving Virtual Assets
(Vienna, March 2026)

The Organization for Security and Co-operation in Europe (OSCE) is a pan-European security body whose 57 participating States span the geographical area from Vancouver to Vladivostok. Recognized as a regional arrangement under Chapter VIII of the United Nations Charter, the OSCE is a primary instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation in its area. Its approach to security is unique in being both comprehensive and co-operative: comprehensive in that it deals with three dimensions of security – the human, the politico-military and the economic/ environmental. It therefore addresses a wide range of security-related concerns, including human rights, arms control, confidence- and security-building measures, national minorities, democratization, policing strategies, counter-terrorism and economic and environmental activities.

PARTICIPATING STATES: Albania | Andorra | Armenia | Austria | Azerbaijan | Belarus | Belgium | Bosnia and Herzegovina Bulgaria | Canada | Croatia | Cyprus | Czech Republic | Denmark | Estonia | Finland | France | Georgia | Germany Greece | Holy See | Hungary | Iceland | Ireland | Italy | Kazakhstan | Kyrgyzstan | Latvia | Liechtenstein | Lithuania Luxembourg | Malta | Moldova | Monaco | Mongolia | Montenegro | Netherlands Norway | Northern Macedonia Poland | Portugal | Romania | Russian Federation | San Marino | Serbia | Slovakia | Slovenia | Spain | Sweden Switzerland | Tajikistan | Türkiye | Turkmenistan | Ukraine | United Kingdom | United States of America | Uzbekistan

ASIAN PARTNERS FOR CO-OPERATION : Afghanistan | Australia | Japan | Republic of Korea | Thailand
MEDITERRANEAN PARTNERS FOR CO-OPERATION: Algeria | Egypt | Israel | Jordan | Morocco | Tunisia

Office of the Special Representative and Co-ordinator
for Combating Trafficking in Human Beings

FOLLOWING THE MONEY 2.0

A Collaborative Approach to Human Trafficking Investigations Involving Virtual Assets

OSCE Organization for Security and Co-operation in Europe

Table of Contents

List of Abbreviations

AFC	Anti-Financial Crime (legislation)
AML	Anti-Money Laundering
BTC	Bitcoin
CAD	Canadian Dollar
CFT	Countering the Financing of Terrorism
CEX	Centralized Exchange (platform) for Virtual Assets
CSAM	Child Sexual Abuse Material
CSE	Child Sexual Exploitation
CSEM	Child Sexual Exploitation Material
DeFi	Decentralised Finance
DEX	Decentralized Exchange (platform) for Virtual Assets
EFIPPP	Europol Financial Intelligence Public Private Partnership
ETH	Ethereum
EUROPOL	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FI	Financial Institution
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Intelligence Unit
ICT	Internet Communication Technology
IP	Internet Protocol
IVAN	Illicit Virtual Asset Notification
IWF	Internet Watch Foundation
KYC	Know-Your-Customer
LE	Law Enforcement
LEA	Law Enforcement Authority/Agency
LTC	Litecoin
MICA	Markets in Crypto Assets Regulation
ML	Money Laundering
MLAT	Mutual Legal Assistance Treaty
NGO	Non-Governmental Organization
NRA	National Risk Assessment
OE	Obliged Entity
OSCE	Organization for the Security and Co-operation in Europe
OTC	Over-The-Counter
PF	Proliferation Financing
PP	Public Partnership
PPP	Public Private Partnership
R&D	Research and Development
SAR	Suspicious Activity Report
SDN	Specially Designated National
STR	Suspicious Transaction Report
TFR	Transfer of Funds Regulation
THB	Trafficking in Human Beings
TL	Terrorist Financing
USDC	United States Dollar Coin (stable coin)
USDT	United States Dollar Tether (stable coin)
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VIR	Voluntary Information Record
VPN	Virtual Private Network
WTV	Welcome to Video
XMR	Ticker symbol for Monero

List of Key Terms

Anti-Financial Crime (AFC) Legislation	A term used in this report to encompass regulations pertaining to anti-money laundering, countering the financing of terrorism, proliferation financing, as well as sanctions.
Blockchain	A decentralized, distributed digital ledger that securely records and links transaction data in chronological blocks, making the data transparent, immutable, and resistant to tampering across a network of computers.[1]
VASP	A legal entity or business that professionally provides one or more virtual-asset services – such as custody, trading, exchange, administration, or advisory services related to crypto-assets.[2]
Darknet	Encrypted network within the Internet that can be accessed only by specialty software or certain software configurations. Darknets may be small, intended just for specific people or much larger, like the popular Tor network.[3]
Decentralised finance systems	Blockchain-based financial networks that enable peer-to-peer transactions, lending, borrowing, and other financial services without intermediaries like banks, using smart contracts on a public, permissionless blockchain.[4]
Egmont Group	International network of Financial Intelligence Units (FIUs) that facilitates the exchange of information and cooperation to combat money laundering, terrorist financing, and other financial crimes.[5]
Fiat currency	Government-issued money that has no intrinsic value and is not backed by a physical commodity, but derives its value from the trust and legal decree of the issuing government.[6]
Financial Intelligence Unit	A central unit with a national mandate to analyse reports received from an entity with an obligation to report suspicious activity related to financial transactions suspected to be linked to illicit activities, such as money laundering. In the event where the FIU finds grounds for the suspicion, they alert law enforcement authorities.
Know-Your-Customer (KYC)	Mandatory process where financial institutions and other businesses verify a customer's identity and assess their associated money laundering risks before establishing a business relationship.
Law Enforcement (LE) Law enforcement agency (LEA)	A government agency that is responsible for the enforcement of the law. Law enforcement agencies have powers, which other government subjects do not, to enable them to fulfill this responsibility. A national example of a national LEA is the Federal Bureau of Investigation (FBI) while an example of an international LEA is Europol.
Over-the-counter (broker)	Direct, off-book transactions conducted between two parties, typically a buyer and a seller, facilitated by a broker or dealer, rather than executed on a public exchange. Instead of routing orders through order books visible to all market participants, OTC desks match large trades bilaterally, often negotiating price, settlement, and other terms privately.[8]
Peer-to-peer service	Platforms or systems that let users trade or transfer digital assets directly with each other – without a central intermediary.[9]
Politically Exposed Person (PEP)	An individual who holds or has held prominent public positions, and because of their role, is considered to be at higher risk for involvement in bribery, corruption, or other financial crimes.[10]
Smart contract	A self-executing agreement in which the terms of the contract are written into lines of code. Smart contracts use distributed ledgers like blockchain to document and validate contract transactions without the need for oversight by a central authority.[11]
TOR web browser	Free, open-source web browser that routes internet traffic through the Tor network – a series of volunteer-run relays – to help hide IP addresses, encrypt traffic, and shield online activity from tracking and surveillance.[12]
Wallet	A digital tool that allows users to securely store, manage, transact, and interact with their cryptocurrency assets. It consists of a pair of cryptographic keys: the public key acts as an address, while the private key – known only to the user – unlocks the wallet.[13]
Web3 (ecosystem)	A version of the internet that uses a decentralized architecture rooted in blockchain technology to give users ownership and control over their data, digital assets, and online interactions.[14]

Foreword

Efforts to prevent and tackle human trafficking have long focused on the role of the criminal justice practitioners, largely downplaying an essential element of the crime and criminal intent – the money. The last decade has seen a shift with several OSCE participating States and financial institutions taking measures particularly focusing on the traditional banking system in detecting and disrupting illicit financial flows, which criminals continue to utilize at scale.

The OSCE's 2019 paper Following the Money: Compendium of Resources and Step by Step Guide to Financial Investigations Related to Trafficking in Human Beings, demonstrated how financial institutions, regulators, and law enforcement agencies can identify human trafficking patterns through transaction monitoring, risk indicators, and public–private partnerships. That analysis underscored that financial footprints are among the most powerful tools for uncovering trafficking networks, protecting victims, and holding perpetrators accountable.

As financial ecosystems evolve, however, so do traffickers' methods. The rapid expansion of virtual assets and blockchain based technologies has created new opportunities for anonymity, speed, and cross border movement of funds—features that are attractive to criminal networks engaged in human trafficking. Cryptocurrencies now facilitate a range of trafficking related activities, from payments for sexual exploitation of children to the financing of cyber enabled scam compounds where trafficking victims are forced into criminality. These developments intersect with broader patterns of exploitation, including the recruitment of vulnerable individuals through deceptive online job offers and the use of advanced technologies, such as Artificial Intelligence, to scale criminal operations.

This paper examines how cryptocurrencies are being misused within trafficking economies, the regulatory and operational gaps that enable such misuse, and the urgent need for coordinated and proactive responses. As in the 2019 paper, here we propose guidance in six steps, including a list of red-flag indicators to support financial intelligence and institutions and criminal justice practitioners in the detection of trafficking related to both digital and financial footprints of victims and trafficking perpetrators.

As digital finance continues to expand, understanding the nexus between cryptocurrencies and human trafficking is essential to building effective, accountable, and victim centred strategies for prevention, protection, and justice.

I hope this paper provides useful guidance for all stakeholders in both understanding the role of the virtual assets in trafficking crime and serves as a tool for effective detection and prevention in implementing these recommendations.

Dr. Kari Johnstone
OSCE Special Representative and Co-ordinator
for Combating Trafficking in Human Beings

Acknowledgement

The present paper was prepared by the Office of the OSCE Special Representative and Co ordinator for Combating Trafficking in Human Beings (OSR/CTHB) under the dedicated and visionary leadership of Tarana Baghirova, Programme Officer.

The OSR/CTHB extends its sincere appreciation to the Tether compliance team, Leonardo Real, Matthew Alexander, and Jonathan Dupont, for their excellent collaboration in drafting and analysing data, and to Daniel Shonfeld and Joseph Mari for their expert input and peer-review of this guidance document.

The OSR/CTHB also wishes to thank Nadja Long for her written contributions particularly in examining Anti-Financial Crime (AFC) regulations and partnership models and to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Research Institute of Digital Forensics at the Law Enforcement Academy of the Republic of Uzbekistan, Chainalysis, TRM Labs, and Elliptic for their valuable written input and case studies.

These inputs and case studies significantly enriched the guidance by grounding the analysis in real world practices, illustrating emerging trends, and demonstrating how different actors are responding to trafficking risks in the virtual asset ecosystem.

Introduction

In 2019, the Organization for the Security and Co-operation in Europe (OSCE) published a report titled *"Following the Money: Compendium of Resources and Step-by-Step Guide to Financial Investigations Related to Trafficking in Human Beings"*.[15] Organized by the Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, this project was the culmination of efforts to enhance detection and prevention of illicit financial flows related to trafficking of human beings (THB).

The first section of that report, the Compendium of Resources, was a synthesization of more than 20 publications into a comprehensive guide for practitioners to detect THB in the financial sector. Indicators from a wide range of jurisdictions were compiled, analyzed, and grouped into categories to form a single resource. The second section, a Step-by-Step Guide to Financial Investigations Related to Trafficking in Human Beings, provided necessary guidance to frame the financial investigations in 11 steps. The 2019 report purported to demonstrate the approach of following the money including through better alignment cross borders, given the complex and multi-jurisdictional nature of THB- related financial investigations.

As the second edition of OSCE's approach to detecting and preventing illicit financial flows stemming from trafficking in human beings, the present report examines how digital technologies are re-shaping the criminal landscape – particularly with regards to trafficking into cyber scam operations and online sexual exploitation of children – and aims to address existing barriers to successful financial investigations where Virtual Assets (VA) are involved.

In addition to a comprehensive list of financial red-flag indicators, this document also includes social red flags – non-financial indicators related to human trafficking in cyber-scam operations – in an effort to promote awareness and prevention by financial institutions and criminal justice practitioners on the modus operandi of criminals.

The proliferation of global social media, together with the more recent emergence of VAs, has proven a boon to savvy cyber criminals. While Chainalysis data released in 2025[16] showed approximately 0.14 percent of on-chain transaction volume in 2024 attributed to criminal activity, its 2026 report[17] shows an 85 percent growth in cryptocurrency flows to suspected human trafficking services, largely based in Southeast Asia, reaching a scale of hundreds of millions across identified services. According to Internet Watch Foundation, of 1,678 instances of child sexual abuse imagery, 1,067 offered payment via virtual currencies across sites where payment options were visible.[18]

IWF Data: Type of cryptocurrency and other payment types encountered in 2024

Payment Type Analysis	Total Payment Instances
Others (Money Transfer Services)	474
Bitcoin	386
Others (Virtual Currency)	380
Litecoin	96
Ethereum	92
Dogecoin	55
Visa Card	39
Mastercard	36
Paypal	30
USDC Coin	29
DAI	29
Others (Credit Card)	24
Discover	3
Diners Club	3
Email	2
Total of 15 items	**1678**

Payment Group Analysis	Total Reports	Total Payment Instances
Virtual Currency	518	1067
Money Transfer Service	291	506
Credit Card	42	105
Total of 3 items	**851**	**1678**

Although these figures have been improving in recent years, more collaboration between public and private sector stakeholders with regard to the responsible uses of technology is needed to address niche risks and evolving threats.

Borderless online products and services give transnational criminals an asymmetric advantage over law enforcement, especially where multiple jurisdictions are involved, by enabling them to more easily conceal unlawful transactions and disguise the true owners of suspicious financial flows. Furthermore, the use of anonymising technologies such as VPNs and the continued presence of dark web marketplaces add layers of complexity to the monitoring of such activities.[19] However, as described further in the paper, when public and private sectors collaborate VAs and related technologies also have the potential to enhance law enforcement outcomes in ways that traditional financial investigations cannot.

This report aims to raise awareness about emerging criminal typologies involving online child sexual exploitation and THB for the purpose of forced criminality where criminals increasingly use virtual assets, as well as to provide guidance to financial institutions in six steps to address any existing barriers to successful related financial investigations when VAs are involved.

The report is organized into six steps for conducting financial investigations involving VAs.

Step 1: "Understanding Virtual Assets" provides a high-level overview of VAs with a key focus on a few key VA that are frequently used by criminals.

Step 2: "Understanding Trafficking Modus Operandi" reviews key terminology related to trafficking for forced criminality and online child sexual exploitation including through case studies to highlight emerging criminal typologies.

Step 3: "Red Flag Indicators" outlines financial and non-financial indicators for two specific typologies – online child sexual exploitation and trafficking for forced criminality in cyber scam operations, as well as best practices for using a system of both red and yellow flags.

Step 4: "Identifying Partners" discusses the roles of stakeholders from both the public and private sectors in investigating virtual assets, as well as explores different types of existing partnerships as promising practices.

Step 5. "Gathering Evidence" demonstrates the different sources of digital and financial evidence available to criminal justice practitioners to investigate virtual assets related transactions.

Finally, **Step 6. "Recovering Assets"** explores the existing asset recovery process, with an emphasis on stablecoin freezing and reissuance mechanisms.

STEP 1

Understanding Virtual Assets

In any trafficking of human beings (THB) investigation involving virtual assets (VAs), law enforcement must first understand and confirm the types of relevant VAs . What most VAs have in common are deposit addresses and transaction IDs, or "hashes," which serve as identifiers; but they may differ in other capabilities, such as the ability to trace and freeze. It is also important to understand the different types of virtual asset service providers (VASPs) that trafficking perpetrators may utilize to conceal and launder funds. While some criminal schemes involve outright fraudulent platforms, others use more regulated VASPs that are obligated to comply with regulations pertaining to anti-money laundering (AML) and countering the financing of terrorism (CFT), proliferation financing (PF), as well as sanctions (collectively referred throughout this report as Anti-Financial Crime, or AFC regulation). These businesses are generally better able to share information with law enforcement and may have investigation teams dedicated to such collaboration.

Decentralized finance (DeFi) offers further advantages to criminals, as these platforms are automated by code and are not typically governed by AFC regulations like other VASPs. Having some basic knowledge of VAs will enable law enforcement agents to better communicate with VASPs regarding the details of their cases (e.g., deposit addresses, transaction hashes, etc.) when requesting asset freezes, including the blockchain tracing that led them to a specific VASP. Since financial investigations involving VAs are time sensitive, such efforts will increase the likelihood of a successful asset freeze or recovery.

Types of Virtual Assets

There are many different ways to categorize and describe the wide range of available VAs, which the OSCE's recently published "Decoding Crypto Crime: A Guide for Law Enforcement"[20] covers in greater detail. This report will briefly introduce selected VAs based on their reported use by trafficking perpetrators.

Bitcoin

The Bitcoin network was initiated in January 2009. Originally introduced as "a purely peer-to-peer version of electronic cash that would allow online payments to be sent from one party to another, without going through a financial institution,"[21] Bitcoin has become both a powerful financial innovation, by enhancing global payments, as well as a transformative monetary innovation, by introducing the first scarce (non-copiable) digital asset. Unlike most other VAs, Bitcoin uses a "Proof of Work" consensus mechanism that incentivises anonymous volunteers ("miners") to secure the network. This ensures that the number of bitcoins (BTC) that can ever exist is capped at 21 million, which is why some refer to it as "digital gold."[22] By contrast, stablecoins may be created ("issued") upon the receipt of fiat deposits, for which there is no physical limit.

Bitcoin now has a market cap of US$2.24 trillion, making it the seventh largest asset in the world by market cap, behind only Alphabet (Google), Amazon, Apple, Microsoft, NVIDIA, and gold. Throughout bitcoin's history, however, high transaction fees and price volatility have led to it being used more as a store of value than for payments. Bitcoin was the first blockchain and spawned the VA industry, which now has a combined market cap of US$3.9 trillion. Although the illicit use of bitcoin has been decreasing relative to other VAs[23], its benefits for cross-border transactions have not gone unnoticed by criminals. In 2025, the U.S. Department of Justice reported the seizure of roughly $15 billion in bitcoin connected to a major scam compound in Cambodia that had been operating extensive romance scam schemes.[24] This action marked one of the largest cryptocurrency seizures to date. In 2019, the Financial Action Task Force (FATF) updated its Recommendations to ensure that VAs (including Bitcoin) and VASPs are covered by domestic AFC regulations.

Today, Bitcoin can be purchased from thousands of different service providers, using a variety of methods. Some VASPs enable their users to purchase VAs using their bank account, credit or debit cards, while others only allow VAs to be exchanged for other VAs (e.g., buying BTC with stablecoins, such as USDT, etc.). Although transactions on the Bitcoin network are publicly available, enabling the tracing of funds using specialized software, Bitcoin can generally only be seized by law enforcement when it is being stored with a third-party service such as a VA exchange or when law enforcement gains control of the private keys for a VA wallet.

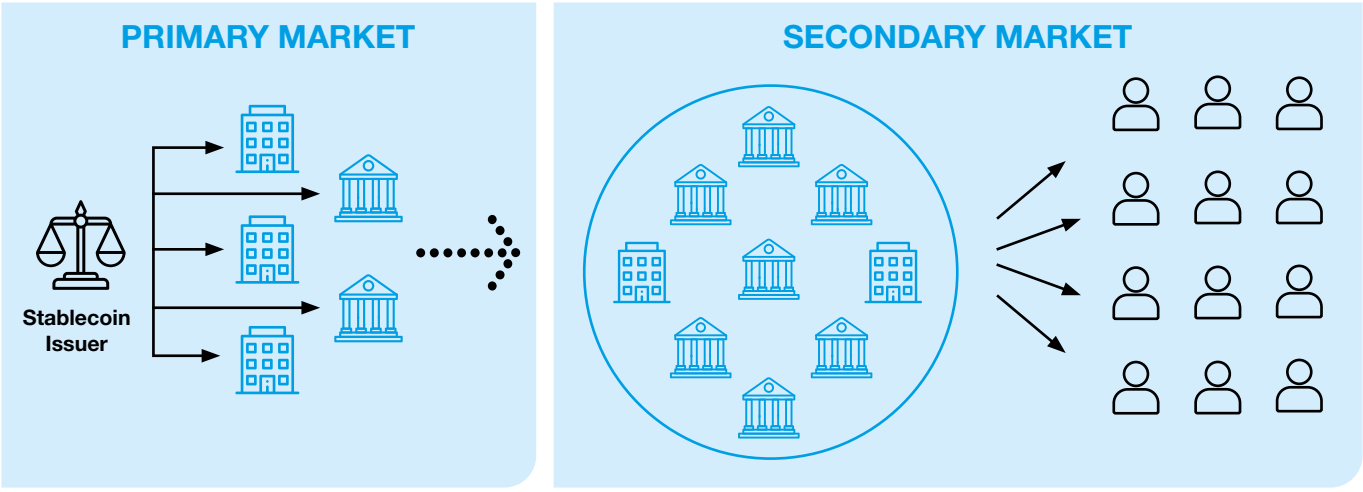
Stablecoins

This category of VA was created in 2014, in response to the strong market demand for a financial product with the transactional benefits of bitcoin or other VAs, but with a "stable" value that was denominated in, or "pegged to," a fiat currency, most often the US dollar. The first stablecoin, Tether, or USDT, was created in October 2014, and operates as a "fiat-backed" stablecoin that is fully backed by Tether's reserve assets. Alternative stablecoin business models such as "algorithmic" or "crypto backed" have since been launched, but centrally issued "reserve-backed and fiat-denominated" stablecoins (e.g., USDT, Circle's USDC, etc.) are by far the most popular, both in terms of tokens in circulation and transaction volumes.

The business model of reserve-backed, fiat-denominated, centrally-issued stablecoins is relatively straightforward. After completing the know-your-customer (KYC) onboarding process mandated by AFC regulations, customers may request to either be "issued" or to "redeem" stablecoins at the 1:1 pegged rate, less potential applicable fees. When being issued stablecoins, a customer sends a fiat payment to a stablecoin issuer, and then receives the purchased stablecoins to a deposit address that the customer provides to the issuer. When redeeming stablecoins, a customer transfers the tokens to an address controlled by the stablecoin issuer, and then the customer receives a fiat payment from the issuer to a bank account controlled by the verified customer:

As Illustrated in Figure 1, transactions between stablecoin issuers and their KYC-verified customers make up the primary market, while the secondary market comprises all subsequent transactions of issued stablecoins across many different trading pairs and exchanges. Primary market transactions are priced at the specified 1:1 pegged rate (less applicable fees), while secondary market prices are fully determined by market-based price discovery. Unlike Bitcoin or other VAs, stablecoins do not operate as standalone blockchains themselves, but instead leverage a range of existing blockchain technologies where on-chain transactions are fully traceable. This mitigates technology risks, as issues with any single blockchain would not nec-

Figure 1:
Primary versus Secondary Market



essarily threaten either the business model nor the reserve assets of a stablecoin issuer. The daily volume of stablecoin transfers is significantly larger than any other VA, with the top two stablecoins often accounting for more than 47% of the value of all VA transfers since 2020. According to Chainalysis, Stablecoins now account for the majority of all illicit cryptocurrency transaction volume – 63% of all illicit flows – reflecting a significant shift in how criminal networks move and store value. This development mirrors a broader market trend in which stablecoins have become central to the crypto ecosystem overall, with year over year growth in stablecoin activity reaching approximately 77%, making them one of the fastest expanding segments of the digital asset landscape.[25] A unique feature of stablecoins that is particularly relevant to law enforcement is the ability of centralized stablecoin issuers to freeze and re-issue funds that have been traced to illicit activity. This process is further explained in Step 6.

Other Virtual Assets

Apart from Bitcoin and stablecoins, thousands of other VAs have been created with varying characteristics. Launched in 2015 and 2017 respectively, Ethereum and Tron are two other widely traded VAs that are more programmable than bitcoin, allowing for greater smart contract functionality. By enabling blockchains to automate programmatic behaviour in a trustless manner, smart contracts are the technology behind Defi, which allows users to swap one VA for another or lend VAs, amongst many other uses. The launch of Ethereum and Tron preceded the explosion of other VAs, many of which rely on their smart contract technology. Criminals typically seek to convert illicit funds into VAs that are easier to convert into fiat, but they may also leverage less popular VAs to further obscure the flow of funds before ultimately cashing out their illicit gains.

Ethereum and Tron are also the two most popular blockchains on which stablecoins operate. USDT, issued by Tether, currently operates on twelve different blockchain protocols, while USDC, the stablecoin issued by Circle, operates on nineteen.[26] Each blockchain protocol has different technical capabilities and niches within the blockchain industry. Some blockchains allow for faster or less expensive settlement, or they may be useful in specific Defi markets.

Privacy enhancing VAs have also been developed, which have additional cryptographic software that can further obscure transactions.[27] Such VAs, (e.g. Monero), are generally regarded as higher risk because their transaction history is not publicly visible like other VAs. An increasing number of darknet markets have stopped accepting Bitcoin and only accept Monero.[28] Privacy enhancing VAs have been banned by some regulators including in the EU through the Markets in Crypto Assets (MiCA) regulations[29], and some VASPs choose not to list privacy enhancing VAs due to their higher inherent money laundering (ML) risk.

Like Bitcoin, but unlike centrally issued stablecoins, other VAs such as Tron and Ethereum can generally only be seized if they are being stored on a third-party platform or if law enforcement gains control of the private keys to a given VA address.

General Uses of Virtual Assets

VAs are used in large part for speculative trading and investments, to build value and information transfer systems, and are increasingly relied on for general cross-border trade. While relatively few VAs have experienced sufficient growth to be considered "systemically important"[30] by global regulatory bodies, this may soon change as major industries continue their adoption of VAs. By 2024, there were an estimated 560 million VA users around the world, representing 6.8% of the global population. Approximately 72% of these users are younger than thirty-four, signaling bright prospects for future growth.[31] One early use-case of VAs is remittances, where funds can be transferred abroad much cheaper and faster than traditional remittance service providers. VA remittances were expected to increase from US$295 billion in 2021 to US$428 billion in 2025.[32] Although stablecoins were initially used primarily for trading bitcoin and other VAs, adoption is growing from businesses that engage in more traditional cross-border trade, as well as from individuals outside of the U.S. seeking access to dollar-like products, particularly in countries where the local currency is experiencing a higher-than-normal rate of inflation. The transactional utility of VAs provide valuable solutions to both large enterprises and migrant workers alike.

Anti-Financial Crime (AFC) Regulation & Virtual Assets

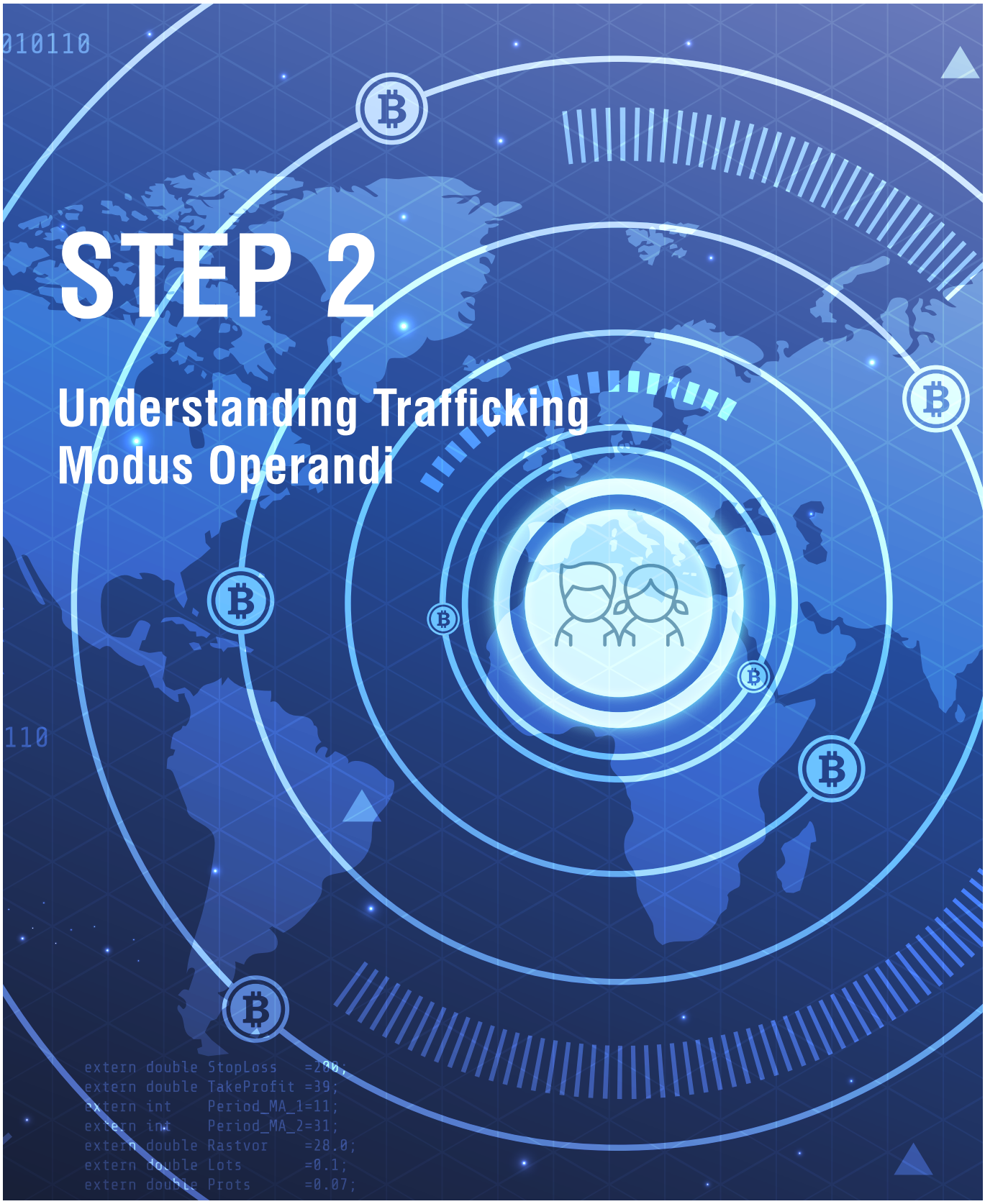
Businesses and other entities that are required to comply with AFC regulations ("obliged entities", herein referred to as "OEs") play an important role in the detection and prevention of crime, including THB. The Financial Action Task Force (FATF) is a global governance body that works to strengthen and standardize AFC laws around the world. Member states of FATF and related regional bodies are required to apply the crime of ML to all serious offences, with a view to including the widest range of predicate offences, or face poor reviews or even listing as grey or black listed countries due to shortcomings in the implementation of regulations.[33] Since the emergence of VAs, regulators around the world have been scrambling to ensure that these assets are either covered by existing AFC regulations that applies to financial institutions, or that appropriate laws are enacted to mitigate the new risks from this industry.

The 2025 FATF update[34] found that while more jurisdictions have adopted laws aligned with Recommendation 15, global implementation of anti financial crime standards for virtual assets remains uneven, with only a small share of countries achieving high levels of compliance and many still struggling to supervise VASPs effectively. Risk assessments have become more common, yet enforcement actions and operational oversight lag behind, leaving significant vulnerabilities, particularly as stablecoins, DeFi platforms, cross chain services, and other emerging technologies expand rapidly. Travel Rule adoption has progressed

on paper but remains fragmented in practice, undermining cross border information sharing and enabling illicit actors to exploit regulatory gaps. To close persistent implementation gaps and ensure that AML/CFT controls keep pace with the speed and complexity of the virtual asset ecosystem, the FATF urges States to shift from formal rule making to active, risk based supervision; fully operationalize the Travel Rule; strengthen enforcement against non compliant VASPs; address emerging risks by applying standards to all actors with control or influence over DeFi and stablecoin arrangements; and regularly update national risk assessments to reflect evolving typologies.

In jurisdictions where AFC regulations exist with respect to VAs, OEs face the same broad AFC-related responsibilities as financial institutions: (1) appoint a compliance officer; (2) develop internal AFC policies; (3) maintain employee training programs; (4) regular reviews and maintenance of AFC programs; (5) customer due diligence (CDD); and (6) travel rule obligations.

From a law enforcement perspective, the responsibility of OEs to conduct CDD is a key source of information and potential evidence. This includes personal identifying information that must be collected before services can be provided, as well as records of their customers' ongoing transaction activity and log-in activity. For example, most VASPs are required to maintain transaction monitoring programs to detect illicit activity on their platforms, so that it can be reported to authorities. While these legal requirements are foundational to combatting ML, there are several limitations that are best mitigated by voluntary collaboration between the public and private sectors. This will be explained in Step 4.


010110
STEP 2
Understanding Trafficking
Modus Operandi
110
extern double StopLoss =200;
extern double TakeProfit =39;
extern int Period_MA_1=11;
extern int Period_MA_2=31;
extern double Rastvor =28.0;
extern double Lots =0.1;
extern double Prots =0.07;

The second investigation step is to understand the nature of money laundering risks and typologies associated with trafficking in human beings (THB) or child sexual exploitation (CSE). Since criminal methods are constantly evolving, it is important that both public and private stakeholders – those in a position to make a difference – be aware of emerging criminal trends. This section will highlight the intersection between THB and CSE, summarize the most recent collection of national risk assessments, explain how digital technologies are being used to facilitate these crimes, and provide case studies of emergent typologies.

Trafficking of Human Beings & Online Child Sexual Exploitation of Children

Defining Trafficking of Human Beings

The Palermo Protocol defines trafficking in persons as a process that combines an act, a means, and a purpose of exploitation. In essence, it covers the recruitment, transportation, transfer, harbouring, or receipt of a person through coercive or abusive methods, such as force, threats, abduction, fraud, deception, coercion, abuse of power, or exploiting a person's vulnerability, as well as payments made to control another person. These actions must be carried out for the purpose of exploitation, which the Protocol specifies to include at minimum sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude, or the removal of organs, although this list is not comprehensive or limited. This definition forms the international legal foundation for identifying and combating trafficking in human beings worldwide, including OSCE commitments.[35]

The EU Anti-Trafficking Directive[36] expands on the minimum exploitative purposes of trafficking by adding the exploitation of criminal activities, or the exploitation of surrogacy, forced marriage, or illegal adoption.

Defining Online Sexual Exploitation of Children

Online sexual exploitation of children (OSEC) refers to situations where technology is used as a tool to sexually exploit children. It covers any exploitative act that is connected to the digital environment at any stage, whether the abuse happens directly online or technology is used to facilitate or record it. It is best understood as an umbrella term for sexual exploitation involving a digital component, rather than a separate category of exploitation in itself.

Child Sexual Abuse/Exploitation Material (CSAM/CSEM)

Child sexual exploitation material (CSEM) is an umbrella term that captures all sexualized material depicting children or material that is exploitative to the child despite not explicitly depicting the sexual abuse. Child sexual abuse material (CSAM) refers to any content that depicts sexually explicit activities involving a child[37]. Both CSEM and CSAM can take various forms such as videos, images, audio files, written story lines, or any other potential forms of recording. Since the majority of CSAM/CSEM is exchanged, bought, and sold online, these illicit marketplaces can easily span many jurisdictions. The CSAM obtained from various forms of child sexual abuse and exploitation may be used by child sex offenders as admission to communities of like-minded individuals who require their members to share new, unseen CSAM to be accepted into their group, or to view new content.

Summary of THB Data in National Money Laundering National Risk Assessments

As a baseline exercise, the OSCE has analyzed the most recent national money laundering and financing of terrorism risk assessments of 56 OSCE participating States. A National Risk Assessment (NRA) helps countries and financial institutions better understand the predicate offences that generate illicit financial flows, and serves as a foundational step towards an effective risk-based approach to addressing crime. It also informs States' response strategies and helps to prioritize where resources should be allocated.[38] This section summarizes the aggregate findings of NRAs with respect to THB risks.

Nearly three quarters of the reports identified trafficking in human beings as a significant money laundering threat, while almost one quarter of participating States did not reference human trafficking at all in their national risk assessments. The chart below illustrates the geographical distribution of these responses:

Across the 57 participating States, approaches to assessing THB risks in NRAs vary widely, with significant gaps in how threats are identified and classified. Of the 43 countries that included THB in their NRAs, 10 specified the level of threat as "high". A larger group of nine States assessed THB risk as "medium", while a small number rated it as "low" or "medium low".

Overall, the data shows inconsistent recognition of trafficking related risks, with many States either omitting key forms of exploitation or failing to assess their severity, resulting in an uneven regional picture of how THB are integrated into financial crime risk frameworks.

A much larger share – 39 NRAs (68%) – acknowledged virtual assets as relevant to money laundering or terrorist financing. While majority of the examined NRAs do not contain information on the use of virtual assets for trafficking in human beings, several States (i.e. UK) identified the use virtual assets to make payments associated with online child sexual exploitation and abuse.[39] This highlights a major analytical gap: while States increasingly recognize crypto related ML/TF risks, they rarely connect these risks to trafficking related exploitation, even though traffickers are known to use digital assets in certain sectors as further outlined in this paper.

Figure 3:
Number of NRAs mentioning crypto currencies or virtual assets

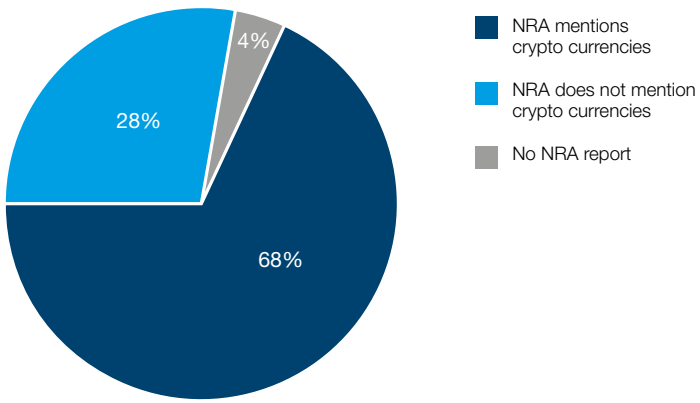
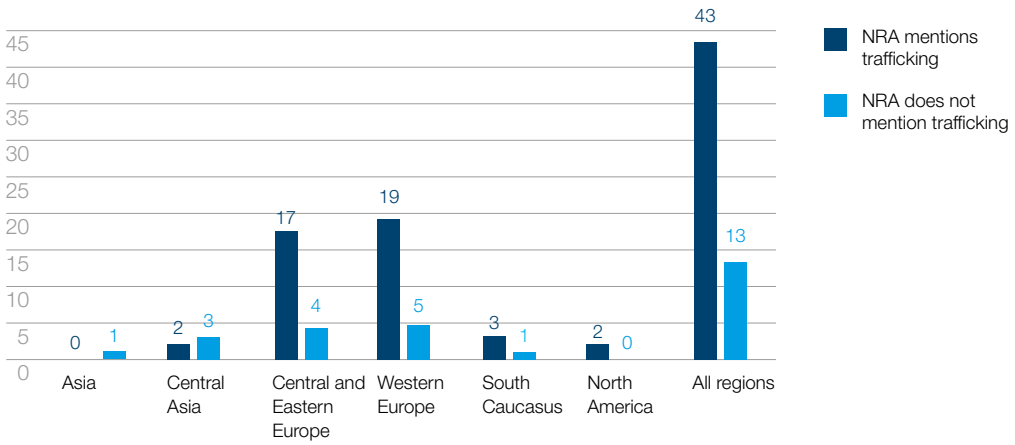


Figure 2:
Number of NRAs mentioning trafficking in human beings as a threat for money laundering (classified by region)



How Digital Technologies Broaden the Criminal Landscape

The internet has led to the emergence and rapid expansion of technology-facilitated THB. When it comes to moving and hiding the proceeds of human trafficking, while the traditional banking system continues to be at risk of misuse, the emergence of VAs has enabled traffickers to anonymously and securely receive their illegal proceeds more easily. While various reports also confirm that illicit funds from THB flow through the traditional financial services sector, often through online services,[40] VAs make it easier to launder and distribute funds between different members of their criminal networks.

Digital technologies have also facilitated the surge of online sexual exploitation of children. Such illicit activity is enabled by the existence of a large number of persons willing to pay to view CSAM, and the minimal investment required to receive CSAM or related payments. The only requirements are an internet connection, some electronic device like a smartphone or computer, and a platform to receive financial payments. With the proliferation of digital technologies, would-be traffickers and exploiters no longer need to be in the same physical location as their victims, and funds can be rapidly moved around the world and across VA platforms to obscure their criminal origin. For example, as reported by the Polaris Project, traffickers are using social media to recruit victims into their operations, and controlling them through restricting access to their social media, impersonating the victim, or spreading lies and rumors online.[41] Individuals are also trafficked for criminal activities, such as into cyber-scam operations and forced into perpetrating online frauds on behalf of organized crime groups.

One particularly pernicious and increasingly common scheme is the trafficking of a certain cohort of skilled individuals and forcing them to perpetrate a so-called "Pig Butchering" scam, the idea being to "fatten up" victims before "slaughtering" them for their assets.[42] Although this term continues to be used, it can be seen to revictimize financial victims and hence this paper will use the term "trafficking for cyber-scam operations."

In such operations, THB victims are forced to perpetrate these scams by building relationships with potential financial victims, often through online dating platforms, social media, or messaging services. Once trust has been gained, the unsuspecting financial victims are introduced to fake investment opportunities, which often involve VAs, and are then persuaded to liquidate traditional financial assets and make large deposits into platforms that can be used to purchase VAs, only for fraudsters to gain control of the funds and disappear. To scale up their operations, organized crime groups often recruit THB victims by the hundreds, or even thousands, to work in facilities dedicated to perpetrating these scams.[43] Such facilities are most often in Southeast Asia, and THB victims with the requisite language and technological skills are particularly vulnerable to being recruited into these scams. While not all scam operation schemes rely on THB victims to perpetuate the scams, some of the most lucrative operations appear to conduct operations through THB.

As reported by Chainalysis, these types of scams grew by nearly 40% in 2024 as the fraud industry has increased their sophistication by leveraging AI in operations for platform development, language translation to recruit both THB victims to scam others and financial victims of fraud, and image and video generation.[44] Of the approximately US$10 billion received by scam accounts in 2024, nearly one third was associated with such schemes. A joint investigation between Chainalysis and the International Justice Mission, an organization dedicated to protecting people in poverty from violence, revealed the growing sophistication of scams with their analysis of "KK Park" in Myanmar, a criminal zone along the border of Thailand. Satellite images revealed many newly constructed buildings where thousands of trafficking victims are reportedly being held against their will:

Figure 4

This operation was only detected after two VA deposit addresses intended for ransom payments were traced back to a Chinese shell company operating out of KK Park. On-chain analysis conducted by Chainalysis revealed the connections between ransom-taking operations and the group's primary business of perpetrating romance scams.[45] With digital technologies, including but not limited to social media platforms, online banking and VAs, having enabled organized crime groups to massively scale their operations, law enforcement must become familiar with these new methods, and also with the potential for collaboration with stakeholders in both the public and private sectors when combatting such crimes.

Emergent Trafficking Typologies & Case Studies

Trafficking in Human Beings for Forced Criminality in Cyber-Scam Operations

The past decade has seen a marked rise in criminals exploiting both adults and children across a wide range of illicit activities. Although this exploitation takes many forms, this paper focuses specifically on trafficking for forced criminality in cyber scam operations, a rapidly expanding phenomenon that has become a central concern for governments, international organizations, and private sector actors worldwide. Organized crime groups have quickly learned to leverage social media and gaming and dating platforms to target individuals with deceptive job ads and false romantic intentions to lure them into locations and compounds to force them engage in defrauding unsuspecting victims. Under the menace of physical, psychological control, harsh penalties, and severe punishments, criminals force victims to scam individuals through gaining and then taking advantage of their trust and affection, including romantic ties, in order to access their cash, bank accounts, and credit cards and invest in fraudulent crypto investments. According to the recently released data by UN and Interpol, at least 300,000 people originating from 66 countries, including from at minimum 19 OSCE participating States have been trafficked in cyber-scam operations in South-East Asia.[46] The Chainalysis 2026 Crypto Crime Report reveals a stark growth of 85 percent of cryptocurrency flows in 2025 to suspected human trafficking services, largely based in Southeast Asia, reaching hundreds of millions of dollars across identified services. In the meantime, the economic impact of scam compounds was estimated at $442 billion in 2025, according to Global Anti-Scam Alliance Report[47].

Trafficking into cyber scam operations is not a simple, single step crime. Instead, these schemes rely on a mix of many different tools, services, and financial channels – some legal, some illegal – to function. The elements of the crime, however, are mostly limited to direct contact with potential trafficking victims. This form of trafficking differs from THB for forced labour because of the illicit nature of the activity that THB victims are forced to perpetrate that imply penalties. Traditionally, the jurisdictions legally involved with instances of THB for the purpose of forced labour have been limited to where the crime is committed. In instances of trafficking for cyber-scam operations, however, prosecuting perpetrators is more challenging as criminal organizations often force their THB victims to scam financial victims in various foreign countries. An additional and key challenge has been a widespread corruption or a lack of appetite to prosecute such criminals in the jurisdictions that host mass scamming compounds. UN Human Rights has described corruption as being "deeply entrenched in the context of these lucrative operations."[48]

The following step-by-step generalized example outlines how trafficking into cyber-scam operations can be perpetrated:

1. Organized crime groups, typically formed in South-East Asia, post false advertisements for employment opportunities that require good international language and IT skills.
2. Persons seeking employment travel for an in-person interview, where they are subsequently kidnapped and brought to a scam factory.
3. The criminal groups train the victim to use social media, messaging apps, and dating apps to approach potential individuals (financial victims), often in more affluent countries.
4. Darknet markets or social media platforms facilitate the sale of packages of social media accounts that already have followers and pictures with comments, as well as fraudulent trading or investment platforms that can be used by organized criminal groups.
5. THB victims are forced to befriend potential financial victims and build a relationship of trust for a period of time before introducing them to a high-yield financial endeavor sometimes involving investment in VAs.
6. THB victims are often forced to operate seemingly real social media profiles with followers, posts, and comments that are meant to convince potential financial victims they are communicating with an individual who is genuinely interested in them.
7. Financial victims send funds from their traditional financial account to a VASP, often a popular and sometimes regulated trading venue, as a first step to introduce funds into the VA ecosystem.
8. Once fiat is deposited to the VASP, the assets are traded for stablecoins or other VAs and then sent to a fraudulent investment platform.
9. The fraudulent investment platform appears legitimate and offers various services to financial victims. Often these platforms publish false information to trick financial victims into thinking that their investments are performing well.
10. Financial victims may even be allowed to withdraw some profits via stablecoins or other VAs back to a VA wallet they control, or to a legitimate VASP, to build trust and persuade the financial victim to send more funds into the fraudulent platform.
11. When maximum value has been extracted from the financial victim, or when the financial victim shows suspicion, the THB victim ceases communications, often deleting all evidence and social media accounts.

Given the complex and increasingly transnational nature of such schemes, it is crucial for public authorities to collaborate across borders. Furthermore, since such schemes increasingly involve VAs, public authorities should also familiarize themselves with this industry and the different types of VASPs. The illustrations below show how numerous stakeholders across multiple jurisdictions may be caught up in such scams. In this example (Figure 5), the scam starts on social media, where the financial victim is persuaded to transfer funds from their bank account to a regulated VASP. Fiat Funds are exchanged for Bitcoin (BTC). BTC is then transferred to a fraudulent platform and further laundered through private wallets and decentralized VA exchanges, before finally ending up in consolidation wallets:

The above example highlights the different stakeholders and their relative abilities to inform local Financial Intelligence Units (FIUs) about potential crimes. Obligated entities (OEs) are required to cooperate with law enforcement and the FIU in the jurisdiction or jurisdictions where the OE is regulated, but not in other jurisdictions.

Figure 6. illustrates how law enforcement agencies that have traced financial victim funds to a VASP outside of their jurisdiction typically must rely on a mutual legal assistance treaty (MLAT) to receive transactional information. As well, FIUs can exchange information using secure channels like the Egmont Secure Web (ESW) or other equivalent networks, based on principles of reciprocity and mutual agreement. These processes can be extremely time intensive, enhancing the criminals' asymmetric advantage and giving them more opportunity to launder funds beyond recognition.

Figure 5
Romance Scams: A Simplified Example

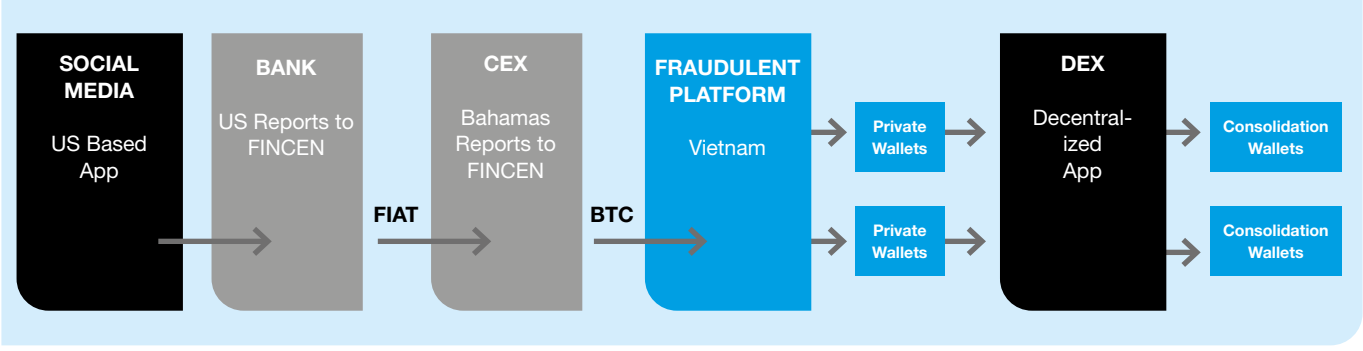
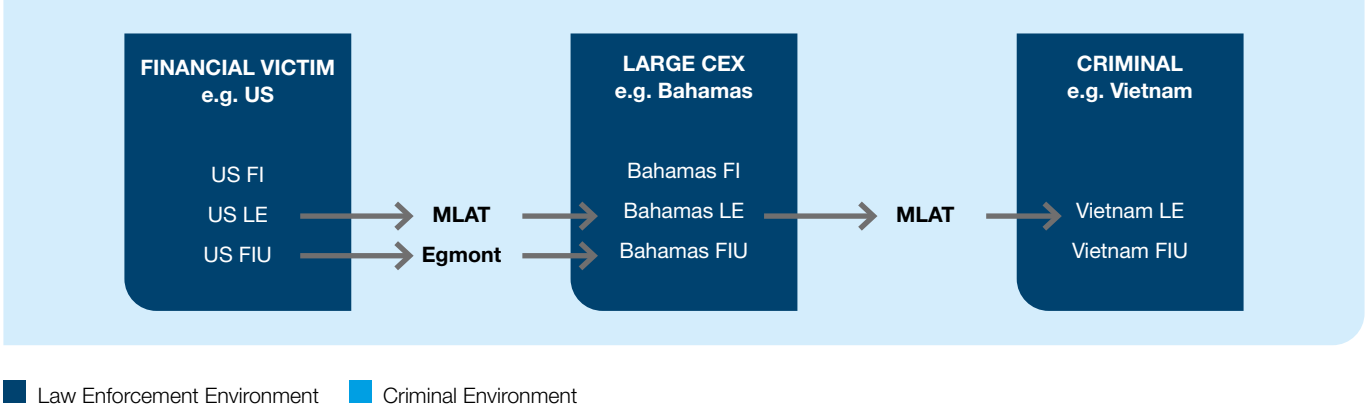


Figure 6
Asymmetrical Environments: Criminal vs LE



Child Sexual Exploitation

Although digital technologies are at the forefront of innovation in payments, they are increasingly becoming a tool used by criminals who exploit children for sexual purposes. As reported by the Internet Watch Foundation (IWF), an NGO dedicated to stopping online child sexual abuse, the number of websites found to be accepting VA payments for sexual content of children has doubled almost every year since 2015. According to IWF data, nearly two thirds of illicit CSEM payments were conducted using some type of VA, although money transfer services and credit cards continue to be used as well. Coinbase, a prominent VASP, has recently conducted an exercise that used IWF data to identify more than 6,500 people believed to be misusing their platform for alleged criminal purposes.[49]

Chainalysis' Crypto Crime Report 2026[50] finds that CSAM producing networks continue to accept mainstream cryptocurrencies, but they are shifting more heavily toward Monero for laundering because of its privacy features. Instant exchangers, services that allow rapid, anonymous crypto to crypto swaps without KYC, have become central to how these groups obscure financial trails. The report also notes that CSAM operations have largely moved to a subscription based business model, replacing pay per content sales with monthly fees typically under $100, which lowers entry barriers for offenders and creates steady, predictable revenue for operators. While criminal groups remain early adopters of new technologies, these trends highlight the need for VASPs to understand evolving abuse patterns and strengthen controls to mitigate associated risks.

Live Online Child Sexual Exploitation

Live online child sexual exploitation refers to the participation of a child in real or simulated sexual activity, alone or with other children or adults, that is transmitted live through internet communication technologies (ICTs) and watched by others remotely. It typically involves children who are coerced or forced by the child sex offender who is requesting and/or directing the sexual abuse, and the trafficker who plays a facilitating role. The abuse may take on both commercial and non-commercial forms; in some instances, a business may be organized with the intent of financially profiting from the sexual abuse of the child victims.

The use of ICTs allows child sex offenders to communicate with traffickers and facilitators around the world who are livestreaming the sexual abuse of children. The child sex offenders watching remotely may then request the sexual abuse of the child and/or dictate how the acts should be carried out, either in advance of the sexual abuse or while it is underway. Even if participating from a distance, however, the role of child sex offenders should never be minimized due to the perverse incentives created by their demand and the harm they cause.

Child victims are sometimes sexually abused by the facilitators in order to satisfy the expected or communicated sexual fantasies of their offending customers. In addition to requesting the sexual abuse of the child and/or dictating how the acts should be carried out, child sex offenders may arrange travel specifically to engage in in-person sexual encounters with children. There is a strong association between the consumption of live online child sexual abuse and subsequent travelling to locations where the children were sexually abused. In some cases, live online child sexual abuse is a way to continue sexually abusing children after having returned from such travels. As a result, live online child sexual abuse may be a precursor or a consequence of transnational child sexual offending. It can also be a staging mechanism for child victims before their eventual exploitation in commercial sex.

Live online child sexual abuse is often transmitted to viewers through "streaming" over ICTs. The term "streaming" refers to the real-time production and transmission of audio and video files in a continuous flow over a wired or wireless internet connection. Since the data is being transmitted instantaneously to the electronic device of the viewer, who can watch and engage remotely while the sexual abuse is occurring, this activity leaves no trace on electronic devices (except possible written conversations), because no file is downloaded or saved onto a hard disk. When the streaming is stopped the material is gone. The content is only available on one occasion and, unless deliberately recorded, leaves no trace on the electronic device once it has been viewed. In this regard, the sexual abuse may be recorded by child sex offenders or the traffickers themselves, and then disseminated or sold online. This adds substantially to the volume of CSAM available online.

The CSAM obtained from live online child sexual abuse may also be used by child sex offenders to join communities of like-minded criminals who exchange CSAM and require their members to share new and unseen CSAM to have access to content. Within such communities, CSAM is considered as a form of currency in itself.

Case Study: Welcome to Video[51]

In March 2018, Jong Woo Son was indicted on nine counts for being the administrator of Welcome to Video (WTV), considered to be one of the largest darknet CSAM marketplaces by volume of content. Welcome To Video hosted approximately 250,000 unique videos (over 8 terabytes of CSAM), with 45% of the videos containing new imagery not previously known to exist. Users accessed WTV in the TOR web browser, where they would register an account to access the website. Videos could only be viewed if the user was registered on WTV. Once registered, users received a unique Bitcoin address to which they sent CAs, in exchange for "points" that could be used to purchase videos. An annual membership to WTV was priced at 0.03 Bitcoin (approximately $350 at the time).

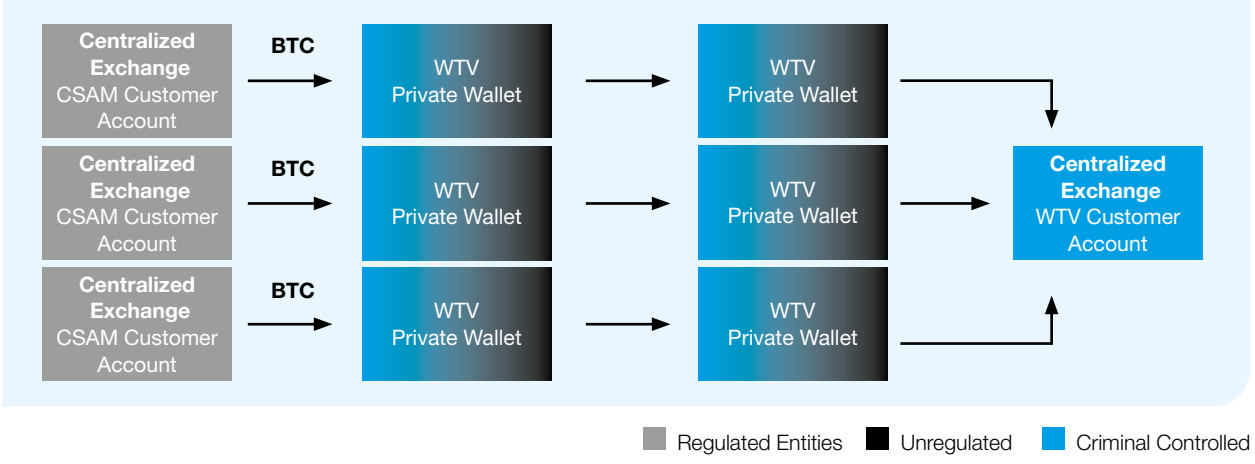
These points could also be earned by uploading content. The more the user's video was downloaded, the more points they earned, enabling them to access and download more content on the website. The website's warning stated, "Do not upload any adult porn" and "only new material would be accepted and checked for uniqueness," which encouraged new and frequent abuse of children. The administrator of WTV was identified when a review of the website's code revealed that widgets of the videos posted to the homepage were not uploaded using TOR or other privacy concealing tools. The unprotected IP address was traced to a South Korean residence. In cooperation with local law enforcement, the internet service provider was subpoenaed to reveal the specific residential address associated with the IP.

Since the funds from registered users moved directly into the website administrator's wallet, only the administrator could access the funds generated by the WTV darknet marketplace. The administrator used crypto-asset exchanges based in South Korea, China, and the United States to convert the Bitcoin into fiat currency. The use of centralized and regulated crypto-asset exchanges is what enabled law enforcement to identify the administrator, since these companies are required to collect a range of information before they can serve their customers. Although law enforcement officers identified two suspects based on this information, it was determined that Jong Woo Son used his father's identity to open multiple accounts at these crypto-asset exchanges. Figure 7. shows the flow of funds of Bitcoin from crypto-asset exchanges to WTV, the administrator, and then back to a crypto-asset exchange.

The post-arrest seizure of Jong Woo Son's computer allowed law enforcement to access and investigate each username and bitcoin payment. Blockchain forensics tools were used to trace the flows of CAs all the way back to the cryptocurrency exchange where a WTV customer had initially bought their bitcoin. Law enforcement agents could then request the relevant personally identifiable information held by the VA exchange. This information included ID documents and photos, residential addresses, email and IP addresses, as well as bank accounts and transaction history. Since many WTV users sent Bitcoin directly to the WTV deposit address, law enforcement were able to easily follow the funds and subpoena exchanges to obtain this information.

These investigative efforts lead to the identification of both uploaders and downloaders on WTV around the globe. In total, more than 7,300 Bitcoin transactions (worth more than $370,000 at the time) were processed. As a result, law enforcement authorities from more than 35 countries collaborated to arrest 337 users, and to rescue 23 minors from sexual abuse and exploitation. The many jurisdictions involved with this case study highlights the need to have appropriate mechanisms for cross-border collaboration between law enforcement and other public authorities.

Figure 7



Case Study: Dark Scandals[52]

In March 2020, Michael Rahm Mohammad, a.k.a. "Mr. Dark," was indicted on nine different counts for being the administrator of a series of websites on both the darknet and mainstream internet distributing extremely abusive sexual content, including CSAM. These websites were identified by law enforcement while investigating a user of Welcome to Video. This known CSAM user sent bitcoin to a wallet address listed on the Dark Scandals website, which featured CSAM and rape videos and provided instructions for accessing them. The website advertised over 2,000 videos and images of "real blackmail, rape, and forced videos of girls worldwide." The customers could receive links to this content in two different ways:

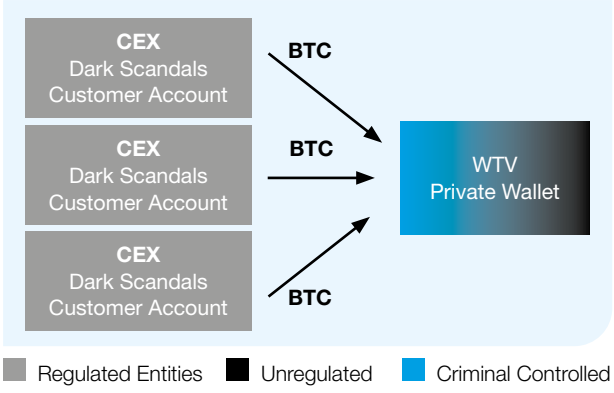
By sending cryptocurrency to the listed addresses on the website or by uploading new videos in accordance with the following rules:

- Uploading unique and "own made material."
- Specifically forbidding fake, amateur, or acted movies.
- Rejection if not portraying sexual violence.

The customers were then instructed to send proof of payment to an encrypted email address listed on the websites (bitcoin@darkscandals.com). Once the payment was completed and verified by the administrator, the user received a downloadable link to the content. As part of their investigation, undercover law enforcement officers sent BTC to these addresses and received downloadable links to CSAM and other abusive sexual content. Figure 8 shows the flow of funds of Bitcoin from CSAM customers' crypto-asset exchange accounts to the Dark Scandals administrator:[53]

By using blockchain forensics tools, law enforcement traced Bitcoin and Ethereum payments associated with Dark Scandals to 303 accounts at eight crypto-asset exchanges. Most of these accounts were either opened solely to send cryptocurrency to Mr. Dark's wallets, or were used to buy and sell other illicit materials on other darknet marketplaces, such as for drugs or stolen identities. Mr. Dark received almost $2 million worth of Bitcoin and Ethereum for administering Dark Scandals. He curated the uploaded content before including the material in the packs sent out to customers, and received approximately 1,650 deposits totaling 188.6631 BTC (around $1.6 million at the time) and 26.724 ETH (around $5,700 at the time).

Figure 8



Case Study: Kidflix[54]

Kidflix, one of the world's largest online hubs for child sexual exploitation, was dismantled in a sweeping international law enforcement operation involving over 35 countries, coordinated by Europol and led by authorities in Germany. Created in 2021, the platform quickly became a major marketplace for child sexual abuse material (CSAM), drawing in 1.8 million users globally between April 2022 and March 2025. The investigation culminated on 11 March 2025 with the seizure of servers by German and Dutch officials, uncovering around 72,000 videos at the time. In total, 91,000 unique videos—many previously unknown to law enforcement—were shared on the site, totaling over 6,200 hours of footage.

Unlike other known platforms of this kind, Kidflix not only enabled users to download CSAM but also to stream video files. Users made payments using cryptocurrencies, which were subsequently converted into tokens. By uploading CSAM, verifying video titles and descriptions and assigning categories to videos, offenders could earn tokens, which were then used to view content. Each video was uploaded in multiple versions – low, medium, and high quality – allowing criminals to preview the content and pay a fee to unlock higher quality versions.

Case Study: Project Shadow[55]

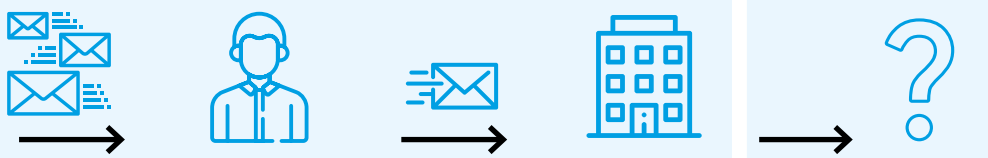
Project Shadow is a public private partnership (PPP) led by Scotiabank that aims to enhance reporting associated with online child sexual exploitation amongst major Canadian banks. This initiative published the following sanitized case study to improve awareness of this issue:

- An underage victim sent a sexually explicit video of themselves to Subject A, whom they met online. Subject A then threatened to circulate the footage of the underage victim if they did not send Subject A $400 CAD. The victim sent the money and reported the incident to the police.
- Law enforcement submitted a voluntary information record (VIR) to FINTRAC, Canada's FIU, regarding an online child sexploitation investigation on Subject A.
- FINTRAC responded in a timely manner by disclosing financial transactions that met the threshold of being suspected to be reclassified to the investigation or prosecution of a money laundering offense.
- The transactions were flagged by the reporting entity as a result of the pre-established indicators developed by FINTRAC pertaining to trends seen in online child exploitation cases, helping FINTRAC meet its grounds to suspect that the transactions were related to child sexual exploitation.
- Figure 9 is a visual representation of the flow of funds, along with sanitized quotes of financial activity from the reporting entity.

Reports received by FINTRAC stated that Subject A was suspected to be involved in the trafficking of internet child exploitation material based on the following trends often seen in such cases:

- Subject A was receiving high volumes of incoming email money transfers from third-party individuals and the reporting entity expressed that the reason for the high-volume transfers was unclear.
- Subject A's account was depleted by sending email money transfers to third party male individuals with various female names indicated as payees.
- The funds were also depleted from Subject A's account via email money transfers ordered to the benefit of a virtual currency dealer. The reporting entity expressed suspicion that Subject A may be using their account at the VC dealer as an intermediary to conceal the flow of funds derived from the distribution of child sex abuse material.
- Although the VIR only provided FINTRAC with a contact name and corresponding email address, FINTRAC was able to provide the law enforcement body with further information, including six account numbers at various Canadian banks, a phone number, and an address and driver's license from the same province.

Figure 9



"… intelligence received … (Subject A) may be involved in the trafficking of internet child exploitation material and sexploitation …

… 18 cancelled and 25 completed incoming EMTs from various males third parties, which list various female names as the payees … cancelled EMTs appear to have related to potential fraud activity …

… depleted via 50 outgoing EMTs … payable to (Virtual Currency Dealer) … (Subject A) may be utilizing his (Virtual Currency Dealer) account as an intermediary to conceal the flow of funds."

"… sent the email money transfer to "scam" (Subject A) … transaction memo reads … "f*** u" …

This case study was disclosed to the appropriate Canadian law enforcement bodies investigating online child sexual exploitation. The FINTRAC money laundering indicators associated with this case study are:

- Insufficient explanation of source of funds
- Email money transfers to third parties with alternate names provided in brackets e.g. jane@example.com (Bambi)
- The reporting entity had indicated a possible link to criminal activity.

Case Study: Uzbekistan CSAM Case

In 2024–2025, Uzbekistan, in cooperation with INTERPOL, conducted a successful operation to identify and detain an individual responsible for the systematic distribution of child sexual abuse material (CSAM) from within the country. The investigation was initiated following a notification from INTERPOL's Crimes Against Children unit reporting the existence of more than 1,000 web pages containing illegal content that had been administered from Uzbekistan for several years.

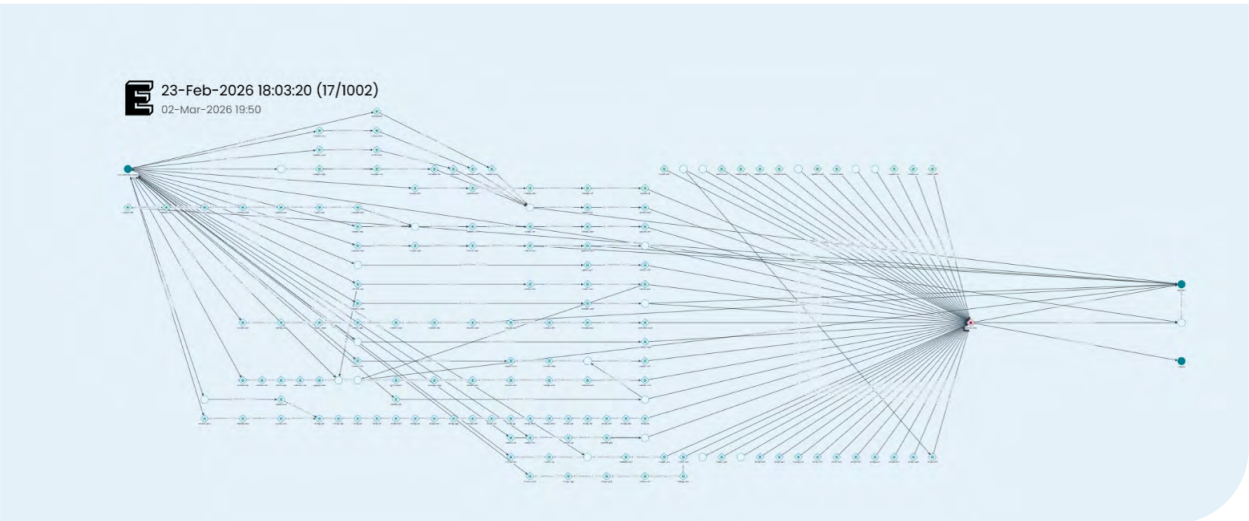
Specialists from the Research Institute of Digital Forensics at the Law Enforcement Academy of the Republic of Uzbekistan conducted a comprehensive investigation using open-source intelligence techniques. Their analysis produced digital evidence that led to the initiation of a criminal case.

The investigation established that the illegal content was hosted on websites in the .fun domain and operated through the hosting provider Hostinger UAB (Lithuania). Hosting services were paid for using cryptocurrency via the Coingate platform. Analysis of transaction records and IP address data provided by the national internet provider Uztelecom enabled investigators to identify the suspect and determine his location in the Bukhara region. With the assistance of state security authorities, the suspect's network activity was placed under traffic monitoring, after which a search was conducted at his residence and multiple digital devices were seized.

A key element of the evidence was the blockchain analysis of a cryptocurrency wallet discovered in the Binance application on one of the seized devices. Transaction history revealed a consistent pattern of incoming USDT payments. Between January 2024 and February 2025, more than 18 incoming transactions totaling over 4,500 USDT were received from multiple senders, typically one to four payments per month. The structure of these payments – fixed amounts ranging from 67 to 947 USDT from anonymous counterparties – indicated systematic monetization of illegal content.

Analysis of outgoing transactions further revealed payments of 664.75 USDT and 282.75 USDT linked to the purchase of hosting services through the Coingate platform, demonstrating that cryptocurrency was used both to receive criminal proceeds and to finance the infrastructure supporting the illegal activity. At the time of the search, the wallet balance was 718.1753 USDT; the funds were immediately seized and transferred to the account of the investigative authority in accordance with legal procedures.

Depending on the stage of the operation, they employed different cryptocurrencies – privacy coins like Monero, Z Cash, and Bitcoin for anonymous hosting payments, and USDT for laundering proceeds – often without any link to regulated crypto platforms.



The use of VAs for the distribution of CSAM

Facilitators of child sexual abuse have long been using VAs under the misconception that these transactions cannot be traced back to them. VAs have been used as a payment mechanism for CSAM content, donating to CSAM platforms, and to enable the uploading of illicit material. Although inroads have been made in disrupting these networks, TRM Labs estimates that over the past two years, there has been at least one VA transaction to a CSAM-related address every two minutes.[56]

The level of sophistication with respect to laundering CSAM proceeds varies across CSAM sellers. The most sophisticated and crypto-savvy CSAM sellers rely on the use of privacy coins such as Monero, which offers robust privacy features. While Bitcoin remains the primary VA for CSAM transactions, vendors are increasingly converting Bitcoin proceeds into Monero to obscure the origin and flow of funds.[57] This conversion is often facilitated by instant exchangers that support Monero transactions, which are typically non-custodial platforms that allow users to swap VAs directly between wallets, often without adequate Know Your Customer (KYC) policies or procedures. CSAM vendors leverage these services to convert Bitcoin into Monero, which can complicate or disrupt the traceability of illicit funds. Nevertheless, instant exchangers may collect some information related to the CSAM sellers (e.g., IP address, email address, etc.). In this regard, although the flow of funds using privacy coins may not be fully traceable, CSAM sellers may leave a digital footprint that can expose them when using instant exchangers that collect some information about their users and comply with authorities (e.g., requests for information).

CSAM sellers typically use a layered approach to launder CSAM proceeds with the goal of obfuscating the flow of funds and cashing out without detection. The primary techniques include:

1. **Converting Bitcoin to Privacy Coins (Primarily Monero)**
   CSAM sellers often receive payments in Bitcoin and quickly convert it to Monero to obscure the trail. Bitcoin transactions are publicly traceable. Monero, by contrast, offers privacy features like stealth addresses and ring signatures, making it much harder, if not impossible, to follow the money.

2. **Use of Monero-Friendly Instant Exchangers**
   CSAM sellers swap Bitcoin for Monero via these services, which create a major laundering layer by bypassing regulated exchanges that would flag suspicious behavior.

3. **Layering through Multiple Transactions**
   CSAM sellers often conduct several hops:

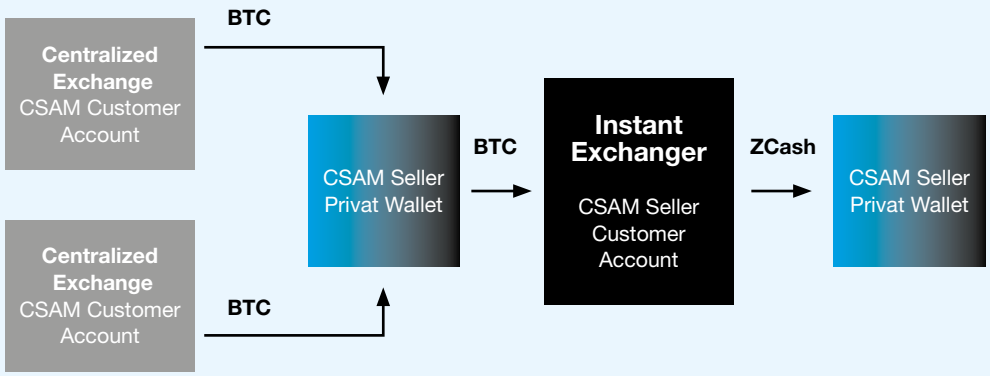
   a. Receive Bitcoin from customers.
   b. Send it to an instant exchanger.
   c. Convert to Monero.
   d. Possibly send Monero to another wallet, then repeat the process by converting back to a more liquid cryptoasset, or eventually convert to fiat currency through no-KYC exchanges, over-the-counter (OTC) brokers or peer-to-peer services.

4. **Use of New Wallets and Addresses**
   Frequent address changes reduce traceability. In this regard, some CSAM sellers propose unique addresses to their customers, making it harder for investigators to build links between VA wallets.

Examples of CSAM-related VA Flows

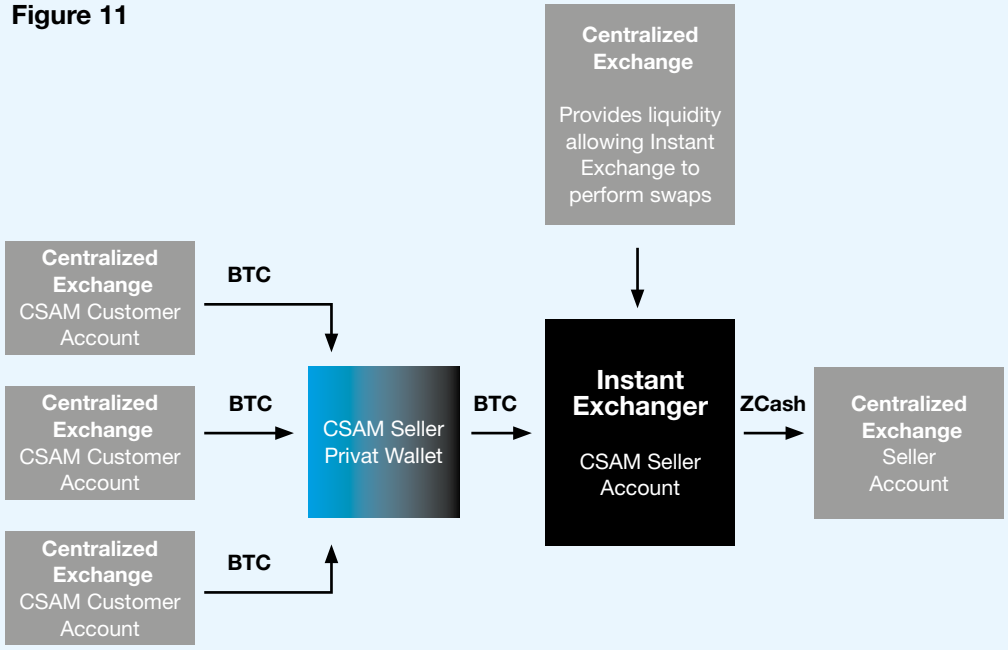
The following illustrations reflect different patterns of CSAM-related VA flows that have been observed by private sector stakeholders:

Figure 10



1. CSAM customers purchase CSAM directly using their exchange accounts
2. The CSAM seller receives payments to private wallets and coverts the Bitcoin CSAM proceeds via an instant exchanger to Zcash, which then becomes untraceable; however, the instant exchanger captures some digital footprint related to the CSAM seller, which can potentially be exploited to identify the seller.

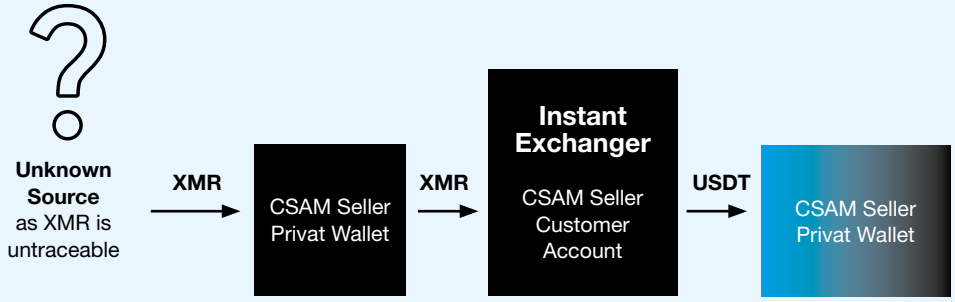
Figure 11



1. The CSAM seller gathers payments from CSAM customer in a private wallet.
2. The CSAM seller then withdraws using a cross-chain bridge by swapping the proceeds to another VA via an instant exchanger.
3. The swapped funds are received from two Obliged Entity exchanges providing liquidity to the instant exchanger.
4. The CSAM seller transfers the swapped proceeds back to one of the Obliged Entity exchanges.
5. In this case, the CSAM seller leaves a footprint via the instant exchanger and the Obliged Entity exchanges, which possess personally identifiable information about the CSAM seller or their associate(s).

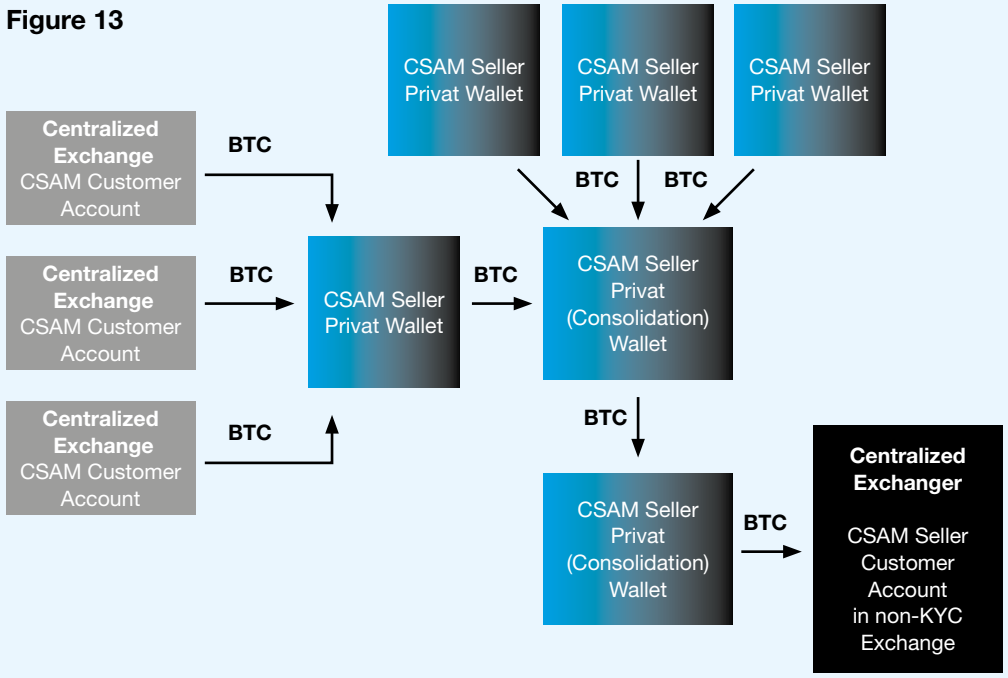
Regulated Entities Unregulated Criminal Controlled

Figure 12



CSAM customers use Monero to purchase CSAM, which makes the source of funds untraceable; however, the CSAM customer converted the Monero assets to USDT via an instant exchanger that captured some digital footprint related to the CSAM customer.

Figure 13



1. CSAM customers fund their wallet with VAs bought on some exchanges;
2. They send VAs to the CSAM seller;
3. The CSAM seller collects payments and periodically withdraws proceeds;
4. The CSAM seller likely controls other CSAM platforms as the proceeds are sent to a common wallet;
5. The CSAM seller transfers some proceeds to other wallets before cashing out at a no-KYC exchange.

Regulated Entities Unregulated Criminal Controlled

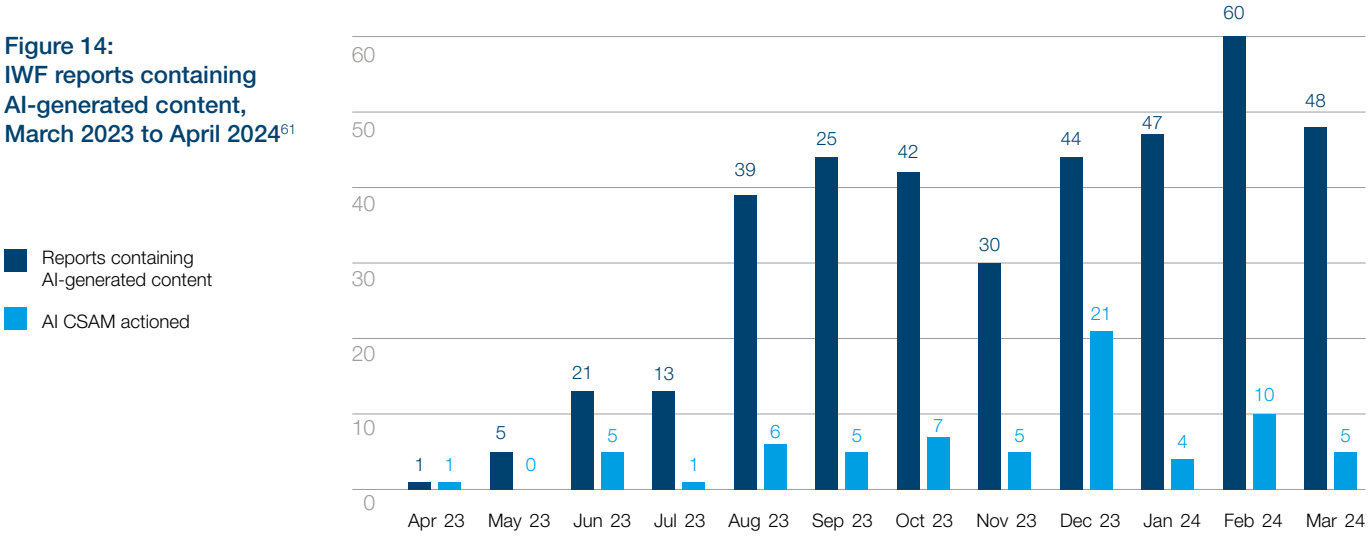
AI-Generated CSAM & other Misuses

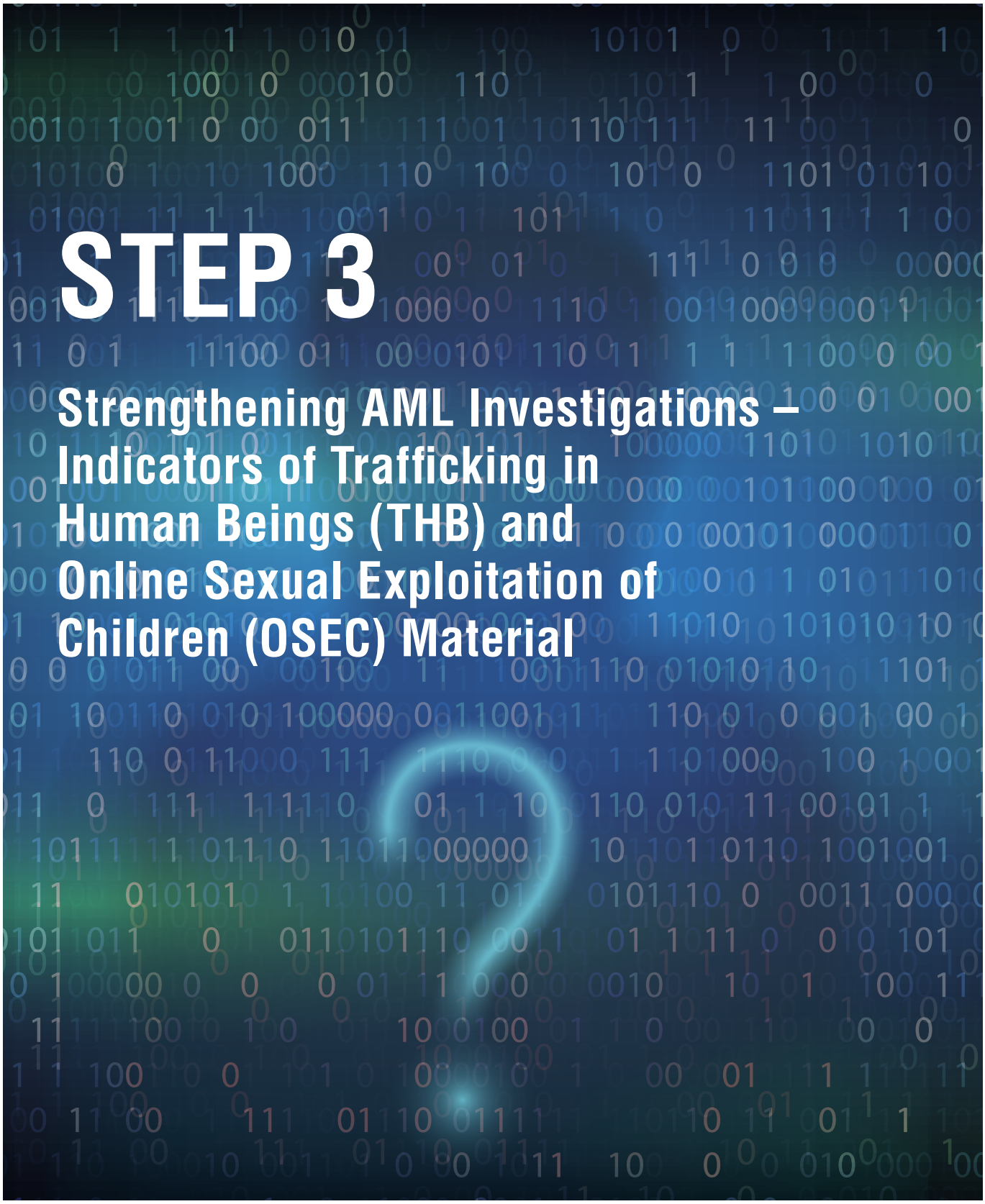
Artificial intelligence represents a new frontier of possibilities for both the production of CSAM and the perpetration of "sextortion" and other sophisticated scams. The Internet Watch Foundation has identified AI-generated CSAM – the use of AI to produce realistic depictions of CSE – as a new and evolving threat.[58] Digital technologies are also increasingly being used to facilitate "sextortion" – threatening or coercing victims to send explicit images online – a crime for which the FBI has reported large increases in child victims in recent years.[59] While these typologies are relatively new and constantly evolving, stakeholders should monitor these areas as more data becomes available.

The Internet Watch Foundation's 2024 update on AI-generated child sexual abuse material highlights the rapid escalation of risks created by increasingly accessible generative technologies. The report underscores how offenders are using open-source and easily modified AI tools to produce synthetic sexualized images of minors, often drawing on real children's photos taken from social media or other online spaces. Traditional detection methods struggle to keep pace, as AI-generated images are unique and difficult to match using existing hashing systems. The IWF stresses the urgent need for updated legal frameworks, stronger platform safeguards, and new technical solutions to identify and prevent the spread of AI-generated CSAM, warning that these synthetic images do not reduce harm but instead create new pathways for exploitation, grooming, and victimization.

The July 2024 update[60] reveals a sharp escalation in AI-generated child sexual abuse material, with more than 3,500 new criminal images appearing on the same dark web forum previously analysed in 2023. The material is becoming increasingly severe, with a growing proportion classified as Category A, showing that offenders are now able to generate more complex and extreme scenarios. The report also highlights the emergence of AI-generated child sexual abuse videos – primarily deepfakes created by overlaying a child's face onto adult pornographic footage – demonstrating rapid advances in generative tools. Beyond the dark web, there is a noticeable rise in AI-generated abusive imagery circulating on the clear web, including on commercial platforms. Alarmingly, perpetrators are also using fine-tuned AI models to produce new synthetic images of known victims and even famous children, further expanding the scope and impact of this form of exploitation.

Figure 14: IWF reports containing AI-generated content, March 2023 to April 2024[61]





STEP 3

Strengthening AML Investigations – Indicators of Trafficking in Human Beings (THB) and Online Sexual Exploitation of Children (OSEC) Material

Background: The Role of Indicators within an AML Investigation

Indicators, also known as flags, of both unusual and suspicious nature, are instrumental to the end-to-end process of the AML investigatory cycle. The relationship between indicators and an investigation are reciprocal, as indicators can be extracted from a completed investigation, while at the same time trigger the commencement of a new investigation. Indicators support the creation and calibration of automated transaction monitoring rules and empower AML investigators with knowledge to not only identify instances of reasonable grounds to suspect money laundering, but also hone in on which predicate offences from which the illicit funds may originate.

Generally speaking, the materiality of an AML investigation can, and arguably should, be evaluated against the indicators that have caused its creation as well as those identified as a result of it. These indicators can be bucketed into 3 (three) categories, which are listed as follows;

1. **Behaviour Indicators**
   These are typically non-traditional financial transaction indicators, which could be found within the information provided for KYC requirements, or the way in which a client interacts with front line bank staff, such as someone speaking on another's behalf.

2. **Transactional Indicators**
   These are indicators that can be observed in a single standalone, or grouping, of financial transactions. An example of this, within the context of THB or OCSE, are transactions sent to known CSAM purveyors. This type of indicator lends itself to more easily be converted into a traditional automated transaction rule.

3. **Investigatory Indicators**
   The final classification of indicators is typically identified during the human portion of an investigation and cannot be readily converted into traditional automated monitoring models. Examples of this type of indicator is information identified outside of internal banking systems via open-source information or external referrals. With respect to THB or OSEC investigations that information could be classified ads on high-risk websites.

Elevating AML Effectiveness Through Defining and Yellow Flags

The concept of a red flag indicator is fairly common within the anti-money laundering field, while the notion of a yellow flag is relatively nascent. The gap in understanding of red and yellow flags largely stems from the absence of a well developed discussion among anti money laundering stakeholders. This discrepancy is further amplified due to increasing tendencies globally, amongst reporting entities, to lean toward reporting red and yellow on an equal basis, without prejudice, out of fear of bringing about regulatory scrutiny for not doing so. Finally, the ever-increasing advancements in technology, such as artificial intelligence, are also inadvertently creating a culture of defensive reporting, which in turn mutes the debate and dialogue needed to further define what exactly constitutes a red and yellow flag.

This last point is an important one and if left unchecked may not only stunt the evolution of red versus yellow flag differentiation but prevent meaningful discussion on structural anti-money laundering reform. This notion is elaborated on in a recent publication from the Royal United Services Institute (RUSI), authored by Georgia Jones, Tom Keatinge, and Kathryn Westmore and entitled The Global Anti-Financial Crime System is Broken. In this publication, the trio suggest that the global focus on submitting more and more suspicious transaction reports has not translated into better outcomes, in terms of identifying and stopping money laundering, but rather created a future in which fear of non-compliance reigns supreme[62].

An often-cited example of the correlation between increased suspicious transaction reporting and lack of effectiveness was found in Italy, where it was reported that in 2010, only 23 out of approximately 37,000 STRs submitted to the FIU were considered useful to a criminal investigation[63]. However, according to UIF (UIF - Unità di Informazione Finaziaria), the Italy's Financial Intelligence Unit, after peaking in 2022, the annual volume of suspicious transaction reports has witnessed a 3-percentage reduction between 2022 and 2023, to end at 150,000 submissions, while the share of subpar-quality STRs dropped 30 percent[64]. The way in which the UIF realized this drop in lower quality reports is multifaceted and includes, but is not limited to, issuing new guidance, providing feedback on reports, and strengthened collaboration. Also, as inferred earlier, another way to support this trend would be through the evolution of differentiation between a red and yellow flag.

Yellow Flags

It can be argued that majority of red flags, on their own, can be more accurately labelled a yellow flag. This notion is supported through existing intelligence guidance offered by leading national financial intelligence units. An example of this is observed through guidance issued by Canada's FIU, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which for years has added the following language to their public-private partnership operational alert series:

"These indicators should not be treated in isolation; on their own, these indicators may not be indicative of money laundering or other suspicious activity. They should be assessed by reporting entities in combination with what they know about their client and other factors surrounding the transactions to determine if there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence. Several indicators may reveal otherwise unknown links that, taken together, could lead to reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence".[65]

In using FINTRAC's recently published Project Shadow operational alert, which focuses on the illicit finances of online child exploitation, to provide examples of yellow flags, the following indicators would lend themselves to be more yellow than red;

- Purchases at vendors that offer online encryption tools, virtual private network services, software to clear online tracking, or other tools or services for online privacy and anonymity, including encrypted email services;
- Excessive payments to online file sharing and hosting vendors/platforms;
- Frequent low-value purchases of cryptocurrencies, particularly privacy coins.
- Purchases or withdrawals of cryptocurrencies using prepaid and credit cards[66].

However, if a more explicit flag, was to be introduced, such as, frequent, low-value funds transfers with references related to child sexual exploitation and/or image and video-based social media platforms, the yellow flags would collectively become red flags. This compounding effect is visualized in the chart below which shows the increasing cumulation of yellow flags, that even without an explicit red flag present, would cross the threshold of reasonable grounds to suspect money laundering.

The idea of a yellow flag is still emerging, but several institutions are already working to integrate it into mainstream practice. The OSCE's approach builds on its recent project with the Swiss FIU (FIAHT), which produced guidance for Swiss financial institutions. ACAMS has also emphasized the value of introducing yellow flag indicators, noting that red flag indicators are often too generic for financial institutions to apply effectively.[67] Yellow flags add an intermediate layer of suspicion that can help determine whether reasonable grounds for a money laundering suspicion exist. When they do not, a yellow flag can simply be recorded for future reference if the client triggers again. Yellow flag insights can also support improvements to automated monitoring systems, allowing red flags to trigger in real time while yellow flags are assessed more holistically.

Red flags for Child Sexual Exploitation

- Cryptocurrency payments made on a recurring basis to one or a group of addresses belonging to the same entity indicative of a possible subscription to a provider of CSAM.
- "Many to One" transfers: Multiple cryptocurrency payments of the same amount to one or a group of addresses belonging to the same entity indicative of a possible CSAM vendor.
- Cryptocurrency payments occur during nighttime hours between 11:00 pm and 5:00 am.
- Frequent purchases in multiples of small amounts of cryptocurrencies.
- Cryptocurrency transactions to sites associated with adult service providers (e.g., escort, pornography, etc.).
- Funds that have been accumulated over time based on multiple small deposits followed by large periodic withdrawals indicative of a possible marketplace withdrawing or transferring profits.
- CSAM cluster withdrawal to mixer, swap service or high-risk exchange (no KYC or based in high-risk jurisdiction), swap profits to privacy coins (Monero, Zcash).
- Cryptocurrency payments made to one or a group of addresses labelled as related to CSAM. Some labelling may distinguish between CSAM and CSAM scams; however, regardless of whether the vendor is real or a scam, the payment of the individual seeking to purchase CSAM demonstrates their intention to obtain CSAM.
- "Many to One" transfers from multiple males in different countries with notes indicative of the purchase of CSAM (e.g., models, content, girls, etc.).

Trafficking of Human Beings for Forced Criminality

THB Red Flags

While these are not financial red flags, the compiled social red flags contain essential information for AFC and criminal justice practitioners to apply to potential victims of THB into cyber-scam operations and help to identify human traffickers and stop their trafficking recruitment processes.

Fake Job Advertisements

Scam compounds recruit people for a wide range of roles, including those responsible for typing and engaging in fake conversations, models, security guards, and coding engineers. These roles require different skill sets, meaning both individuals with very limited skills (e.g., struggling to type) and highly skilled professionals (e.g., those with a PhD in engineering) have been trafficked into these operations. While recruitment methods may vary depending on the target, the presence of multiple red flags from the list below makes it crucial for applicants to stay cautious and thoroughly verify any job opportunity before proceeding.

- Jobs are advertised primarily through social media platforms (e.g., Facebook, Telegram, WhatsApp) instead of legitimate job websites or official company portals.
- Job offers communicated verbally by local recruiters or agents without corresponding public written documentation or company listings.
- Recruiters are overly enthusiastic and pushy, pressuring you to make a quick decision and urging you to leave for the job as soon as possible, without giving you time to think it through.
- Job opportunities specifically targeting individuals with no prior experience travelling or working abroad, making them more vulnerable.[68]
- Direct communication with the company's HR department is restricted, and candidates must rely on recruiters or agents for translations, travel arrangements, and visa processing.
- Job descriptions are vague, with unclear responsibilities, excessive salary promises, and/or no legal employment contract provided before departure.
- The job is linked to high-risk industries, such as gambling, casinos, or hospitality, where exploitative practices are more common.[69]
- The job opportunity was introduced by someone you know—perhaps an old school friend or acquaintance—who claims to be doing well and earning great money at the company to which they want to recruit you, based in South East Asia.

Characteristics of Fake Employers

Trafficking for exploitation in mass-scam operations is predominantly run by Chinese-speaking criminal networks, including individuals from China, Taiwan, Malaysia, and ethnically Chinese groups in Myanmar. As a result, when a company appears to be Chinese-owned and operates in lawless areas, the risk of human trafficking and exploitation significantly increases. These groups typically exhibit the following red flags:

- The employer's registration information is unavailable or inconsistent—for example, company names on contracts do not match those on official websites.
- The employer or its affiliates have been reported in the media for involvement in scams or human trafficking (e.g., Jin Bei hotels in Cambodia).
- The employer's leadership and key staff appear to be Chinese nationals, but the business is registered in another country (e.g., Yongli 永利 compound in Dubai), often in countries with weak rule of law.[70]
- Employers operate in jurisdictions known for weak law enforcement and high corruption.

Common Conditions of Fake Job Offers

The following are common conditions of fraudulent job postings intended to lure unsuspecting victims to criminal compounds:

- Mandatory on-site living arrangements where candidates are required to stay in company-controlled dormitories, limiting their freedom of movement.
- Employers willing to cover travel costs upfront (e.g., flight tickets, visa, accommodation) despite the candidate having limited or no professional skills.
- A significant recruitment fee could be required to secure the job, leaving victims financially trapped and unable to quit, even if the conditions turn out to be different from what was promised.
- Targeted people are specifically asked about their typing speed and written communication skills, which may indicate a role in fraudulent online activities.

Red Flags in Transit Countries

While many scam compounds are located in lawless areas such as Myanmar and Laos' Special Economic Zones, many victims were initially recruited for jobs in nearby countries (e.g., Thailand, Laos) and later transported across borders. Victims often arrive at major airports in transit countries and are picked up by unknown individuals who transport them for hours to isolated destinations. The following red flags have been detected in transit countries:

- Signs of criminal coordination at airports and border crossings, including border officials engaging in corrupt practices, allowing recruiters to bypass normal immigration checks or fast-track entry procedures.[71]
- Transport vehicles picking up victims from the airport and driving them long distances without clear explanations.
- Pick-up codes or vehicles with auspicious license plate numbers favoured by Chinese crime syndicates, such as 8888 or 168.
- Phones and personal belongings are confiscated under false pretences, such as claims that passports are needed for work visa processing.
- Threats and intimidation begin immediately, including warnings not to contact family members or being forced to reassure them that everything is fine.[72]
- Driver changes during long journeys, with drivers visibly exchanging money, suggesting coordination between traffickers.[73]

Red Flags at the Job Site

Many trafficking victims initially did suspect trafficking upon arrival at the scam compounds but sensed that something was off within the first few days. If any of the following red flags are observed, it is crucial for victims to report them as soon as possible to family members, trusted police, or embassies, as early reporting increases the chances of timely intervention and exit.

- Visible presence of weapons both near and within the job location, indicating a high-risk and potentially dangerous environment.[74]
- Passports and other personal identification documents are confiscated by the employer or security guards, leaving workers without control over their legal identity.
- Employees are prohibited from leaving the compound without explicit permission, effectively restricting their freedom of movement.
- Work hours are excessively long (12–16 hours per day) and often scheduled at odd hours, such as overnight shifts to align with U.S. time zones, despite the company being based in Asia.

Financial Red Flags[73]

Indicators linked to scammed victims (hereby referred to as "financial victims") are essential because trafficking for cyber scam operations creates two interconnected victim groups – those exploited in forced criminality and those deceived into sending money – and each group produces different financial and behavioural red flags that reveal different parts of the criminal ecosystem.

Trafficking indicators alone expose the coercion, recruitment, transport, and exploitation of workers inside scam compounds; but they do not capture the financial flows generated by the people being scammed, who often interact with banks, VASPs, and payment providers long before the trafficking element becomes visible.

Financial victim indicators reveal the demand side of the business model: repeated small transfers, sudden investment behaviour, cross border payments to unknown parties, or engagement with high risk crypto platforms. These patterns help identify the financial infrastructure of the scam, map how money moves through mule accounts and laundering channels, and allow earlier detection and intervention. They also expose cross border payment routes that traffickers rely on routes that trafficking indicators alone cannot uncover and provide financial evidence that strengthens trafficking investigations by demonstrating scale, revenue, and organized crime links.

Taken together, trafficking indicators show who is being exploited, while financial victim indicators show how the criminal business model functions and where the money flows, making both indispensable for effective prevention, detection, and disruption of cyber scam trafficking networks.

Indicators for Financial Victims

Large scale organized crime groups are increasingly forcing THB victims to perpetrate online scams against financial victims around the world. Seizing the opportunity to deceive and defraud wealthier individuals, however, requires language and social media skills that THB victims are often more likely to possess. Given the large numbers of financial victims that are susceptible to such scams, providing preventative education to potential financial victims is an important way to both lower their risk and reduce the incentives to recruit THB victims for this purpose. Since global social media and messaging and dating apps often serve as gateways to these illicit practices, these businesses should do more to detect and prevent these types of abuses while also raising awareness among potential victims. The following is a list of common indicators:

- The scammer contacts a target online via social media, a dating or text messaging application by sending a "wrong number" text message.
- The scammer wants to switch to a text messaging application if the initial contact was made via social media or a dating application.
- The scammer sends greeting messages each day to maintain contact and often shares selfies, updates about what they are up to and pictures in various places.
- The scammer shares pictures that convey a sense of luxurious and successful lifestyle (e.g., purchasing expensive items, traveling, and going to events).
- The scammer is typically of the opposite sex and they are typically attractive. In the most elaborate scams, "models" can be hired by the criminal groups to chat with the victim.
- The scammer pretends to live in the victim's country by using Voice over Internet Protocol (VoIP) phone numbers but cannot meet physically for various reasons and always promises to meet in the future.
- The scammer shares selfies and pictures of themselves but does not want to make video calls for various reasons.

- The scammer is very responsive and available to chat at seemingly odd hours due to the difference in time zone.
- The scammer inadvertently texts the victim in another language (e.g., Chinese) and immediately deletes the messages.
- The scammer immediately replies with long (seemingly copied/pasted) messages within a time frame that is not reasonable.
- The scammer shares that they are an entrepreneur, business owner or investor.
- The scammer is passionate about investing and/or trading assets, including cryptocurrency and/or does it as a side job.
- The scammer wants to learn from each other and teach the victim how to invest or trade.
- The scammer shares that they have received their knowledge from a relative or various "sources" they have.
- The scammer appears ambitious and purpose-driven, and they encourage the financial victim to be as well.
- The scammer enjoys discussing investing and/or trading and shows the (fake) profits they make by investing and/or trading.
- The scammer insists or tries to convince the financial victim to invest money and that they would invest/trade and make large profits together.
- The scammer introduces the fake investment and trading platform after soliciting the financial victim's interest and/or acquiring their trust.
- The scammer introduces the financial victim to a website and/or application with a very limited online presence and recognition (e.g., no social media pages, low number of downloads).
- The scammer lends the financial victim some money, a "demo account" or shares their account to try out the investment/trading platform.
- The scammer coaches the financial victim on how to buy crypto-assets on legitimate crypto-asset exchanges, depending on their jurisdiction.
- The scammer lures the financial victim into sending money into their account on the investment/trading platform; however, the financial victim ignores that the account and platform are controlled by the scammer and that no trade occurs on the platform.
- The financial victim may sometimes be offered to fund their account by sending money via their bank account directly to individuals.
- The scammer insists on investing or trading based on their (irregular) schedule and following their guidelines.
- The scammer allows the financial victim to withdraw some (fake) profits to obtain their trust and make the financial victim invest larger amounts.
- The scammer suggests that the financial victim invite friends and relatives to invest and trade with them.
- The scammer belittles the financial victim for not investing enough and highlights some personal struggles the financial victim may have confessed to the scammer (e.g., medical treatment, children's education, etc.) to persuade them to invest more money.
- The scammer questions the financial victim's commitment to the relationship when the victim expresses doubts or complains.
- The platform offers limited time offers, bonuses or incentives to make the financial victim fear of missing out (FOMO) and invest more money without conducting proper research.

- When investing larger or significant amounts of money, the financial victim's account gets "frozen," and the victim is no longer allowed to withdraw money without paying extra taxes or various types of fees, or the platform may indicate that the financial victim has suffered a significant loss and that they need to make up the lost amount.

- The scammer claims that based on their experience, the financial victim will be able to withdraw money again after paying the extra taxes or fees and proposes to help them make up the amount of money when the victim cannot pay the entire amount. However, the platform and everything displayed, such as the victim's account, is artificially controlled.

- The more time passes, the more the victim is urged to pay, otherwise the platform may deduct money from the victim's account.

- The scammer finds various excuses and/or refers the victim to customer service to solve the issue.

- The scammer suggests the victim borrow money from relatives, friends or colleagues and to sell their assets (e.g., home, car, etc.), or to withdraw their retirement savings or take bank loans to invest more money.

- When the financial victim is unable to pay the taxes or fees, the scammer pretends to escalate the victim's case and decide to write off a certain percentage of the initial taxes or fees the victim has to pay on the condition that they provide the remaining percentage. Since the victim believes that they have made high profits, they cannot give it up.

- The scammer tells the financial victim that they owe them money and may threaten the victim in various ways, including sexual extortion if they share sexual content with the scammer.

- The scammer leaves or becomes unresponsive once they know they can no longer financially exploit the victim.

Indicators for Anti-Financial Crime Professionals

Red flag indicators, whether tied to trafficking victims, financial victims, or laundering networks, are also useful for VASPs to translate them into detectable patterns. VASPs should seek to identify such behaviour using transaction monitoring (TM) and blockchain forensics. While TM gives them visibility into suspicious activity occurring within their own platform, the blockchain forensics tools reveal the external network of wallets, services, and laundering channels connected to those transactions. Used together, VASPS can detect financial victim behaviour early, identify laundering patterns linked to trafficking networks, escalate high risk cases for enhanced due diligence, block or freeze transfers tied to criminal infrastructure, and share meaningful intelligence with other VASPs and law enforcement partners. This combined approach is essential because cyber scam trafficking networks operate across borders, platforms, and asset types, making single layer monitoring insufficient to capture the full scope of their activity.

Red Flags Related to Victims

- A customer with no history or background related to crypto-assets suddenly initiates high-value transfers from an existing or newly opened bank account to a centralized exchange (CEX) with no clear rationale or who expresses interest in an investment opportunity leveraging crypto-assets with significant returns.

- A customer with no history or background related to crypto-assets suddenly wishes to exchange a large volume of funds for crypto-assets from a newly opened account at a CEX but demonstrates little or no understanding of crypto-assets.

- A customer mentions that someone reached out to them unsolicited online or through text message and instructed them to exchange fiat currency for crypto-assets at a CEX as well as to deposit crypto-assets at an address supplied by the individual.

- A customer appears distressed or anxious to meet demands or the timeline of a limited investment opportunity on a website and/or application with a very limited online presence, recognition and generally amateurish site design, negative online reviews, and poor spelling or grammatical structure.

- A customer liquidates their bank accounts (e.g., savings account) and attempts to send funds to a CEX in order to exchange the liquidated fiat currency for crypto-assets.
- A customer receives a certain amount of crypto-assets after withdrawing some funds from their wallet, which is subsequently followed by larger transfers.
- A customer whose bank account has been inactive or demonstrated limited activity suddenly begins to show abnormal transactional activity in the form of large and frequent transfers to a CEX (shell) company or individual with which the customer has no apparent business purpose or prior transaction history.
- A customer makes transfers to a CEX with notes indicating "taxes," "fees," "penalties," and/or "AML."

Red Flags Related to Criminals/Scammers

- Funds are received from multiple CEX and often immediately converted into stablecoins through a decentralized exchange (DEX), at an unregulated or noncompliant CEX or a noncompliant OTC broker.
- Initial addresses appear on fake investment, trading websites or social media promising huge returns and that investors will get rich quickly, or on fraud reports/complaints.
- Funds are mixed within consolidation addresses and transactions are sent through multiple addresses showing increasing, larger and round amounts.
- A customer interacts with a DEX associated with relatively high volumes of illicit activity involving cyber scams (e.g., Tokenlon) and cannot explain why they receive decentralized finance tokens from such a DEX and/or addresses associated with cross-chain bridges.
- A customer receives large amounts of crypto-assets stemming from a DEX and attempts to cash out immediately.
- A customer located in a higher-risk, lower-income jurisdiction or poor rural region cannot provide any evidence or logical explanation for their source of funds and/or reception of unreasonably large amounts of money.

Red Flags Related to Money Mules

- Accounts are opened by young individuals, such as university students, who mention that they responded to job advertisements online (often posing under the guise of IT-related positions) offering fees for transferring money.
- Numerous individuals with common biographical identifiers sign up for accounts within a short or the same period of time with no clear apparent purpose.
- Accounts are opened by numerous foreign nationals in higher-risk financial institutions and/or jurisdictions and immediately receive funds within/for a short period of time.
- Inconsistencies between the customer's stated identity information and their online and/or transactional activity in a foreign jurisdiction where they do not appear to have personal or business ties.
- A customer receives a large volume of high-value transfers from multiple addresses to a single recipient address over a short period of time and cannot explain the purpose for such transfers or the source of funds.
- Funds are promptly moved in and out of the bank account or cashed out from the CEX to other accounts or addresses belonging to criminals and/or money mules.
- A customer appears not to have a clear understanding of what the funds in the account are being used for when questioned.
- A customer appears to be totally unaware of funds in the account being transferred in and out when questioned (i.e., stolen identity).
- A customer provides documents that appear to be forged, falsified or stolen.
- A customer uses randomly generated email addresses that just have a string of random numbers and letters or provides other invalid data.

STEP 4

Identifying Partners

Tackling trafficking in human beings by leveraging financial intelligence and investigations requires the involvement of private sector stakeholders in parallel to criminal investigations. This is because law enforcement agencies often require information from financial institutions or other private businesses to conduct their investigations. Whereas one-off, violent crimes must be investigated using physical evidence, the more complex schemes of transnational organized crime groups often leave trails of financial records in different jurisdictions, which are a key source of evidence for law enforcement. This information may be accessed by law enforcement agencies either directly, upon request, or indirectly, via their respective financial intelligence units (FIUs).

For financial institutions, keeping abreast of a shifting criminal landscape will help them better identify suspicions of THB, as well as to conduct more accurate risk assessments and develop more precise red flags to feed monitoring processes and training of dedicated staff. Reciprocally, public authorities may learn useful first-hand information from obligated entities (OE), due to their immediate exposure to the raw data (clients and transactions). For example, blockchain forensics companies often have the newest technology and trained investigators who can assist public and private sector participants with investigations. Building relevant and efficient partnerships will have some key features in common. They will: 1) enable some sharing of information between their members; 2) bring together traditional financial institutions, VASPs and/or other types of OEs, FIUs, blockchain analytics companies, and law enforcement at a minimum; 3) adopt an intelligence-led approach: and, 4) consider the cross-border component.

When virtual assets are involved, requests for information from law enforcement will typically comprise information about a specific deposit address. Both law enforcement and virtual asset service providers typically rely on software from blockchain analytics service providers or free-open source blockchain tracing tools to trace funds in this manner. This section will introduce stakeholders from both the public and private sectors, before exploring various partnership models, such as public private partnerships (PPPs), that have been used to address THB and other forms of transnational crime. THB is a complex crime that is often best addressed by involving multiple stakeholders. The following groups of stakeholders are potential participants for such collaboration.

Stakeholders

Law Enforcement Agencies

Law-enforcement agencies (LEAs) encompass all agencies and personnel tasked with enforcing laws, maintaining public order, and ensuring public safety. Their primary duties include investigating criminal activity and apprehending suspects.[76] Most countries operate multiple tiers of law enforcement, from local or municipal police to national agencies – such as the Federal Bureau of Investigation (FBI) in the United States. The European Union Agency for Law Enforcement Cooperation (EUROPOL) is the law enforcement agency of the European Union, whose mission is to support its member states in preventing and combating all forms of serious international and organized crime, cybercrime, and terrorism.[77] In many OSCE participating States, specialized anti-THB police units have been created. With the increasing digitalization of THB, however, law enforcement mandates related to THB have also expanded to include units responsible for cyber-crime, financial crime, and drug enforcement. Depending on the purpose and focus of a partnership – whether it targets sexual exploitation, forced labour, or criminal exploitation – it is crucial to identify all relevant law enforcement agencies for the purpose of collaboration. In cases where criminal financial investigations involve VAs, it is the responsibility of law enforcement agencies to liaise directly with VASPs to explore options for freezing or seizing assets.

Blockchain Analytics Services

Following the emergence of VAs in 2009, a number of services have been launched that provide blockchain analytics software to both the public and private sectors. Unlike the traditional financial services industry, where transaction information is maintained privately by each institution, information for VA transactions settled on blockchains is available publicly on non-immutable ledgers. This enables a variety of commercial applications to store the numerous blockchains' history and provide additional features that are useful to both the private sector in implementing their compliance policies and to law enforcement for conducting investigations that involve VAs.

Blockchain forensic tools play a crucial role in enabling law enforcement to investigate illicit VA activity, arrest criminals, and seize illicit funds. With the exception of "privacy coins",[78] which are transacted in much lower volumes than stablecoins, Bitcoin, or other VAs, most VAs can be traced using publicly available blockchain data. Since this underlying data is available to anyone who knows how to access it, open-source intelligence sleuths and crypto enthusiasts have been known to track illicit activity such as DeFi exploits and other hacks.

By using "cluster analysis" to group deposit addresses with their corresponding wallets or service providers with a user-friendly interface, blockchain forensics tools make advanced VA tracing and analysis possible with only minimal training and technical expertise. Users can enter deposit addresses and quickly see the exposure profile, transaction history, and counterparties. This enables compliance analysts to quickly adjudicate the risks associated with transacting with certain counterparties, while empowering law enforcement to trace the origins and destinations of illicit VA transfers.

When financial investigations involve VAs, the output of blockchain forensics analysis can be a key aspect of both suspicious activity reporting, as well as in-progress law enforcement investigations. Although the identities of the owners of wallets sending and receiving VAs are generally unknown, law enforcement can use legal processes to request identifying information from VASPs where the VA wallet has been linked to the VASP. The limitations of blockchain forensics are the inability to trace through VASPs and other services, and the difficulty of tracking funds through smart contracts or apps that mix VAs or allow for on-chain trading and conversions to other VAs.

By clustering addresses likely controlled by the same entity, aggregating and visualizing flows of funds, providing a database of clusters associated with known entities, and integrating online and darknet resources to find digital fingerprints related to VA addresses, commercial software applications may help investigators in the following areas:

- Identifying the extent of criminal networks and/or the scale of criminality;
- Identifying and tracing the proceeds of crime or any other assets that are, or may become, subject to confiscation;
- Developing evidence that can be used in criminal proceedings; and
- Submitting freeze and/or re-issue requests to centralized stablecoin issuers

While some blockchain analytics service providers specialize in aggregating and analysing big data sets, other providers specialize in specific use cases like analyzing through mixers or on the ground intelligence. Some examples of reputable service providers are Chainalysis, TRM Labs, Merkle Science, Elliptic, Bitquery, Blockchain Intelligence Group, and Crystal.

Private Sector

Given their size and breadth of transaction activity, banks and other financial institutions have traditionally produced the overwhelming majority of suspicious activity reporting to FIUs. Other OEs include real estate agencies, asset management services, casinos, merchants, jewelers, and other dealers in precious metals. Since 2009, the emergence and rapid growth of the VA industry and its service providers have presented new money laundering risks and challenges for regulators around the world. The use of novel technologies to transfer entirely new forms of value had initially caught regulators off-guard, leaving the VA industry in a state of uncertainty with regards to which rules, if any, would apply to their activities.

Following guidance from FATF in 2015,[79] domestic financial authorities moved quickly to ensure that VA activities were covered under existing AFC legislation. The 2023 Transfer of Funds Regulation (TFR), the EU's equivalent to the FATF's Travel Rule, regulates the customer identity information transfers between VASPs and transactions involving VASPs to and from self-hosted wallets. This improved the traceability of customer identity information in relation to VA transfers within the EU by including VAs within its scope. In essence, VASPs will have to ensure that their fund transfers, in both fiat currencies and VAs, are accompanied by information identifying the originator and the beneficiary. Like other OEs, VASPs will also need to implement procedures to detect whether the information provided by their corresponding intermediary is correct.

The applicability of AFC regulations to VA activities has continued to evolve, with some jurisdictions even enacting new legislation directly aimed at VA activities. But as VA services and technology evolve faster than corresponding regulations, information sharing by VASPs with the private sector and receptiveness of the public sector to receive training from the private sector becomes necessary.

Financial Intelligence Units (FIU)

FIUs are increasingly engaged in guiding the OEs through conducting strategic analysis of THB risks and identifying footprints that perpetrators may leave behind. In recent years, several FIUs across the OSCE region have developed robust guidance on human trafficking, such as Cyprus MOKAS Strategic Analysis Report released in 2022[80], Maltese Financial Intelligence and Analysis Unit's Strategic analysis on Maltese massage parlours and their possible connection to the sexual exploitation of women in 2024[81], and the joint project of the OSCE and Switzerland's Money Laundering Reporting Office (MROS)Financial Intelligence Against Human Trafficking (FIAHT) and the guide released in 2025.[82] Through platforms like FIU.net and the Egmont Group, FIUs securely exchange intelligence with counterparts in other countries, helping to dismantle international THB networks. Moving forward, however, it is important that FIUs work to keep pace with new technologies such as AI and consider automated and instant information transmission capabilities.

NGOs & Survivor led Organizations

Non-governmental organizations (NGOs) have long been active in anti-THB agendas across the OSCE and have made proactive, constructive, and positive contributions towards understanding THB patterns and the development of THB-related policies. Given the nature of their work, NGOs have also been trusted partners when it comes to supporting and engaging with victims and survivors of human trafficking. In this regard, consulting with NGOs and survivor-led organizations has grown in recent years, as both public and private sector agencies acknowledge the role and benefit.

When it comes to the role of NGOs in tackling the illicit flows related to THB, the UK based NGO "Stop the Traffik" has developed a number of initiatives whereby their intelligence specialists assess and corroborate intelligence from multiple sources and channels to produce actionable intelligence to degrade trafficking routes and hotspots. Exploitation Analytics is a consolidation of Stop the Traffik's various data and intelligence products packaged into one integrated offering for commercial organizations that face potential exposure to human trafficking.[83] These intelligence products equip commercial organizations with the tools they need to identify customers and transactions across their operations that are potentially linked to THB or exploitation.

The Child Rescue Coalition is a non-profit organization that rescues children from sexual abuse by developing pro-bono technology for law enforcement that helps to identify, arrest, and prosecute child predators.[84]

Finally, the Anti-Human Trafficking Intelligence Initiative (ATII)[85] is an NGO that provides anti-THB program training, targeted data collection, technology integration, and a variety of other services to help detect THB. These services and data sets help private sector reporting entities to detect transfers related to THB with greater precision and have led to the identification of several suspected trafficking networks.[86]

Partnership Models

Recent years have seen continuous growth in both the number and size of public-private partnerships (PPP), as well as public-public and private-private partnerships at the regional, national, and international levels. Such partnerships pursue a wide range of objectives and may touch many different industries and public agencies. There has been a growing interest in PPPs from AFC stakeholders who have been using this tool to better combat financial crime, especially with regards to law enforcement investigations and outcomes. Today, these different forms of partnerships are used to tackle financial crimes, each helping to exchange and leverage mandates, data, and competencies. Importantly, while this report does publish a variety of red flag indicators, it is also meant to foster closed-door collaboration and knowledge-sharing between the private sector and law enforcement, so that criminals are not also made aware of the latest developments. Public-public partnerships have also been established to enable information-sharing between public entities that are sometimes located in different jurisdictions and are integral part of an AFC framework where each stakeholder brings an added value and highlights the cross-disciplinary and cross-dimension of serious and organized crime, such as THB.

Public-Private Partnerships

PPPs have long been an implicit feature of global AFC efforts, given that the private sector is ultimately relied on to provide timely information to their respective FIUs. But these broadly legislated reporting responsibilities represent only the tip of the iceberg when it comes to the potential for effective collaboration between public and private sector stakeholders. This is especially true in the context of THB, where financial complexity and the involvement of multiple jurisdictions may frustrate law local enforcement efforts. Efficient PPPs will have several key features in common: 1) enable some sharing of information between their members; 2) bring together FIs and/or other types of OEs, FIUs, and LEAs at a minimum; 3) adopt an intelligence-led approach, and 4) consider the cross-border component (even if the PPP is national).

First and foremost, PPPs build trusted communities amongst partners that are not necessarily used to working together. A better understanding of each community ultimately enhances prevention and enforcement, even if PPPs only exchange strategic information and not specific information about individuals or cases. It is therefore important to bring stakeholders for both prevention and investigation to focus on a common goal and to reflect on common difficulties in combating criminal activity, such as legally permissible processes to share information between large companies in the public sector, between private and public sectors, and between public sector actors across national borders.

PPPs help build an up-to-date and consolidated picture of specific crime phenomena. OEs are thereby prompted to file more focused suspicious activity or suspicious transaction reports (SARs/STRs), while FIUs and law enforcement agencies update their knowledge of trends and innovative data management techniques, or receive personal data feeding into ongoing or future investigations. In practice, members of PPPs can elaborate new red flags, modify internal monitoring procedures, prioritize new investigations or analysis, and educate potential victims. By pulling public and private information together, PPPs can also decide to focus structurally over a limited period on certain emerging aspects or on innovative projects. New areas of discussion include, for example, the rise of certain types of money laundering risks linked to the changes occurring in criminal activities during the COVID-19 pandemic, the risk inherent to new forms of financial services such as e-IBANS, the effect of an increase in trafficking in vulnerable persons (children and women in particular) due to the war in Ukraine, new ways to target financial victims, or new modus operandi of circumvention of restrictive measures/sanctions.

Furthermore, by participating in PPPs FIUs may: increase trust with OEs; provide more structured feedback to OEs to improve FIU risk apprehension; and discuss with law enforcement agencies how to fine tune analysis reports to improve subsequent investigations amongst other benefits.

PPPs in the Context of THB

PPPs have grown in number and scope across the OSCE region. These partnerships entail cooperation between investigative authorities and OEs and serve as a crucial pillar in combating financial crime and maintaining security. Europol's recently launched practical guide for operational co-operation between investigative authorities and financial institutions provides in depth analysis of co-operation mechanisms and divides them into three interconnected objectives. First, it enables authorities to uncover new leads by tapping into financial data and insights, which can initiate or redirect investigations. Second, it facilitates the collection of critical evidence – transaction records, suspicious activity reports, and other financial intelligence – that strengthens ongoing cases. Lastly, this partnership plays a preventive role, helping to identify and neutralize emerging threats before they escalate, such as by freezing assets or halting suspicious transactions. These functions often reinforce one another, creating a dynamic and responsive approach to tackling illicit financial activities.[87] While such approaches help to address enforcement of AFC strategies, PPPs should also focus on educating the public: to them avoid becoming victims of THB for the purpose of scams or becoming financial victims. In both cases public sector actors specializing in social media, job recruitment, dating apps, and messaging apps should collaborate with law enforcement to find ways to educate the public about THB and financial fraud risks.

There have already been several PPPs formed specifically to address THB. The Banks Alliance Against Trafficking[88] is a series of working groups in which banks, LE agencies, and other experts have collaborated to draft red flag indicators and toolkits for detecting and combating THB. These resources are shared with wider stakeholder groups, such as the Egmont Group of FIUs. Another example is Project Protect, an initiative led by the Bank of Montreal to increase the number of suspicious transaction reports filed by major Canadian banks.[89] The International Center for Missing and Exploited Children is another organization that partners with leaders in the financial industry to disrupt the economics of child sexual abuse material (CSAM) businesses.[90] ECPAT Sweden is a children's rights organization that works to combat child sexual exploitation through raising awareness and distributing useful information to stakeholders, such as their "Project Indicators" Report, which highlighted common characteristics of payments for live streamed child sexual abuse.[91]

The Harcourt Programme, launched in 2023 in Ireland, is a pioneering collaboration between BPFI, An Garda Síochána, STOP THE TRAFFIK, Ernst and Young (EY), and stakeholders from across the financial services sector aimed at dismantling the financial infrastructure that enables THB. Its mission revolves around preventing exploitation through heightened awareness, detecting illicit activity using data and technology, and supporting law enforcement in securing convictions while easing the burden on survivors. Anchored by three strategic pillars – Awareness, Collaboration, and Technology and Data – the initiative raises public and professional consciousness through survivor-focused campaigns, fosters united cross-sector partnerships, and utilizes cutting-edge tools to identify suspicious financial behavior. As part of its growing momentum, the Programme launched its Project Aware in 2025, a nationwide campaign dedicated to amplifying awareness efforts and mobilizing collective action against modern slavery.

PPPs in the Context of Crimes Involving Virtual Assets

The Illicit Virtual Asset Notification (IVAN) PPP is a channel for US government, international government, and industry entities (VASPs)[92] to share information related to the illicit use of VAs with the aim of disrupting digital crimes. This PPP is designed to facilitate borderless collaboration by allowing users to upload and search VA deposit addresses, to enable VASPs to check for matches in their platform or for connections between their customer transactions to high-risk addresses and to canvass all partners for related information. The trusted third party operating this platform is MITRE, a not-for-profit corporation committed to the public interest that operates federally funded R&D centres on behalf of U.S. government sponsors.

There are also private-to-private organizations being organized to combat crime typologies, such as the Crypto ISAC. Announced in May 2024, this group is a not-for-profit organization that enables information sharing between members in order to protect and enhance trust in the VAs, blockchain and Web3 ecosystem. The Crypto ISAC is supported by industry-leading companies that are shaping the crypto ecosystem. It provides a secure platform for information sharing to help members protect and improve infrastructure, to coordinate response to incidents, and to address emerging threats. For example, the Crypto ISAC has brought together large VASPs and stablecoin issuers in order to discuss how to best share information about crypto=asset addresses that have received funds directly from victims of THB for the purpose of scams. The Crypto ISAC will also collaborate with governments around the world to address region specific threats.

Coinbase has launched the Tech Against Scams coalition with industry players like Match Group, Meta, Kraken, Ripple, Gemini, and GASO to combat online fraud and financial schemes. This partnership aims to protect and educate users, emphasizing that scams are a tech-wide issue, not limited to social media, crypto, or finance.[93]

Other PPPs in Europe

Launched as a pilot project in 2017, the Europol Financial Intelligence Public Private Partnership (EFIPPP) was the first transnational PPP for the sharing of financial information in Europe, and has since become a core project of Europol and its partners.[94] Permanent members of the EFIPPP include Europol, the Institute of International Finance (IIF), and the European Banking Federation (EBF). The organization has three types of members – LE, FIUs, and OEs (typically financial institutions) – that work together on specific topics. Think tanks (e.g., the Royal United Service Institute), international bodies (e.g. the FATF), supervisors (e.g., the European Banking Authority), and academia (e.g., the United Nations University, Center for Policy Research) round out the EFIPPP community.

The governance of the EFIPPP is structured in layers that enable an efficient decision-making process while ensuring the regular delivery of actionable outputs for its members. Since its inception, the EFIPPP has proven flexible in commencing discussions on emerging criminal patterns such as crimes boosted by COVID-19 and the circumvention of sanctions. Its working groups enable members and observers to discuss the financial aspects of the most pressing predicate offenses - such as THB - and draft new typologies, red flags or other resources to be integrated with internal monitoring systems.[95]

PPPs may also be created as distinct legal entities, such as the Centre of Excellence in AML of Lithuania. This Non-Governmental Organization has a separate budget from the national FIU and is the first PPP in Europe to operate as a separate institution.[96] It is organized similarly to the EFIPPP, with different fields of expertise, and according to the priorities of its members (e.g. restrictive measures). In particular, the Center of Excellence offers training and support with regards to identifying risks, with membership covering a wide range of stakeholders in both the public and private sectors. Another example is the Cooperation and Coordination Group (CCG), launched by the Latvian

FIU in 2018.[97] The CCG in Latvia has a flexible membership structure that includes, depending on the issues at stake, investigating bodies; the Prosecutor's Office; the State Revenue Service; OEs under the national AFC legislation; and in some cases supervisory institutions. While also serving as a forum for general feedback between FIUs and OEs, CCG meetings are generally focused on operational information and have led to several cases being solved.[98] The CCG is regulated such that the operational documents and data shared cannot be used as evidence, as such, but can serve informative purposes, which can be followed up by more formal procedures.[99]

On a larger scale, the Dutch FIU set up the Netherlands' first PPP in 2019, the Fintell Alliance, and has since made considerable investments in developing PPPs at the national level. The Fintell Alliance was launched with the participation of four major banks in order to exchange knowledge to improve these banks' transaction monitoring and the quality of suspicious activity reporting.[100] Two other specialized PPPs operating in The Netherlands are the Serious Crime Task Force (SCTF), and the Terrorist Financing Task Force (TF-Task Force), which both operate under the umbrella of the Financial Expertise Center (FEC).[101] Within the FEC, the groups exchanging information include: the Central Bank of The Netherlands (De Nederlandsche Bank), the Tax and Customs Administration, the Financial and Tax Crime Investigation Service (FIOD), the Dutch FIU, the National Police, the Public Prosecution Service, and the Netherlands Authority for the Financial Markets.[102] In the PPPs mentioned above, members exchange operational information and typologies, as well as contribute to different joint projects.

PPP Opportunities & Challenges

Above all, PPPs can generate shared understanding and build trusted communities amongst partners that may not be used to working together. Some OEs may already be familiar with one or more LE agencies due to their direct and ongoing sharing of requested operational information, but all stakeholders can benefit from greater collaboration with regards to the information that LE agencies receive indirectly, through their respective FIUs.

PPPs may also help to keep AFC stakeholders well-informed regarding a shifting landscape of criminal activity. OEs may be prompted to file a higher volume of or more focused suspicious activity reporting, while FIUs and LE agencies can update their knowledge of trends, new data management techniques, or even receive personal data that can support ongoing or future investigations. The sharing of red flag indicators may help OEs to fine-tune their internal monitoring procedures. The flexibility of PPPs enables stakeholders to quickly address specific ML risks that may emerge, whether due to COVID-19, new forms of financial services such as e-IBANS or crypto assets, or the increase of THB risks due to the war against Ukraine.

When PPPs facilitate the sharing of operational information, the criminal justice response may be considerably accelerated. This is an especially critical factor when tackling organized crime. One example is the European Ports Alliance, a PPP launched in 2024 to bring stakeholders together to address illicit activity around ports, a hotbed of organized criminal activity.[103]

There are also numerous challenges involved with launching a PPP. No matter how worthy the objective, or how willing members are to coordinate, the inherent differences between public and private sector contexts may create trust issues between stakeholders. For many OEs, complying with all relevant AFC rules and regulations is a significant cost, and may still involve considerable uncertainty. PPPs should be structured so that the private sector can participate without adding unreasonable costs or commitments.

Another challenge to PPPs sharing information is the need for an appropriate legal framework, and an understanding of any data protection rules that may apply. For example, inappropriately sharing personal data from LE to OEs could lead to de-risking and privacy violations. Conversely, OEs must understand their reporting obligations to ensure that only appropriate and reliable information is shared with FIUs and LE. The issue of data protection was front and center during recent negotiations of the new EU AML legislative package. The European Data Protection Board (EDPB) is an independent body working to ensure "consistent application and enforcement of data protection law across the European Economic Area."[104] In March 2023, it sent letters to the European Commission, Council, and Parliament, asking for the deletion of specific provisions introduced by the Council which allowed, in some cases, for the sharing of operational information in "partnerships for information sharing."[105]

Finally, PPPs can become victims of their own success. Early improvements to LE outcomes may cause the size and number of PPPs to grow such that it could dilute the quality of their output. It is important that PPPs work to manage and maintain their existing partnerships without stretching themselves too thin. Although more cooperation is needed in general, this should only happen if it makes sense for all stakeholders. Some additional PPP best practices will be included at the end of this report.

STEP 5

Gathering Evidence

The fifth investigation step is to gather evidence from available sources. This may include social media companies, financial institutions, or various types of VASPs. While the legal requirements regarding the sharing of information may vary, many large service providers have internal teams who are dedicated to collaborating with law enforcement. As explained in "Decoding Crypto Crime: A Guide for Law Enforcement," there are four key considerations when collecting information in a VA-related investigation: (1) whether the transaction was recorded on the blockchain, (2) which VASPs or financial institutions were involved, (3) the size of the transaction, and (4) the type of VA.[106] Since the victim may not always be able to provide all of this information, law enforcement may need to leverage information that can be provided by the following stakeholders. This is especially important where there is the potential to identify more victims and prospective victims.

Social Media/Dating/Employment Recruitment/Messaging Companies

Social media, dating, employment recruitment and messaging apps have become a vital tool for criminals to recruit potential THB victims and financial victims. Whether through fake job advertisements posted on sites like Facebook, or fake profiles on online dating platforms, global social media companies offer organized crime groups unparalleled access to prospective victims around the world. As the typical starting point from which trust is gained, these platforms may possess demographics statistics, chat histories, contact lists, or other personal information that can help shed light on complex scams. There is mandatory sharing of such information in certain areas (e.g., violent crime, terrorism, etc.), but this is not present in the scam space. Despite the possible legal hurdles and privacy concerns, the voluntary sharing of certain scam-related information may be of great value to law enforcement and even victims. Social media companies may possess information that can help law enforcement identify more victims of a particular scam, which may be the difference between whether stablecoin issuers are able to freeze criminal assets and ultimately return funds to victims. Importantly these companies also have a connection to their user base, which creates an opportunity for education in order to prevent victimization for THB for the purpose of scams or financial fraud. One example of such an initiative is "Know2Protect," a collaboration between the U.S. Department of Homeland Security and major social media companies that involved using free ad credits to target at-risk children and their parents to inform them of CSAM risks.[107] This campaign achieved significant results in its first year of operation, generating over 683 million online impressions, 128 victim disclosures, and over 90 investigative leads.[108]

Financial Institutions

Before the emergence of VAs and VASPs, traditional financial institutions such as retail banks were the primary sources of information pertaining to financial investigations related to THB. Having long been subject to AFC legislation, including the "Travel Rule," banks are required to maintain comprehensive records. They may possess information about sudden liquidations of traditional financial assets followed by outgoing transfers to VASPs from financial victims, or of incoming transfers from VASPs to bank accounts controlled by organized crime groups. This can be helpful when law enforcement are trying to identify additional victims in a large scale scam. Like social media companies, financial institutions may also be able to pair transactional information with demographic statistics, which could be used to target at-risk subjects in a preventative awareness campaign.

Virtual Asset Service Providers (VASPs)

The general application of AFC regulations to VASPs that require data retention standards for customer information, transactional information and regulatory reporting, entails that VASPs may possess information about deposits received from the bank accounts of financial victims or as a result of money laundering by criminals, and also about the movements of these funds once they have been deposited to the platform. For example, such deposits may first be converted into a stablecoin or other VA before being transferred to other VA wallets that are controlled by fraud groups. Funds may be laundered through multiple layers of VASP accounts before being transferred to private wallets or further mixing services. Fortunately, most large VASPs have dedicated investigation teams that regularly work with law enforcement to trace or freeze funds. Further, the recent application of the "Travel Rule" to the VA industry enhances the transaction information that is available to law enforcement.

STEP 6

Recovering Assets

The sixth and final step of a criminal financial investigation involving virtual assets (VAs) is to coordinate any potential asset recovery with the appropriate stakeholders. Since banks or other traditional financial institutions may be involved in the flow of funds to or from virtual asset service providers (VASPs), they will also be included in this section, alongside VA exchanges and stablecoin issuers.

Coordinating with Traditional Financial Institutions

Many financial fraud schemes involving VAs will also have touchpoints in the traditional financial sector, both on the victim side, as well as through accounts controlled by criminal groups. In situations where illicit proceeds are traced to financial institutions such as banks, law enforcement will typically be required to produce a court order known as a Mareva injunction before the bank will take any action to freeze the assets. The ability to obtain such an injunction, however, may vary across jurisdictions.

Coordinating with Virtual Asset Exchanges

Most major VA exchanges employ investigation teams who are tasked with, among other things, responding to inquiries from law enforcement and coordinating actions such as freezing assets and filing suspicious activity reports when appropriate. These platforms typically offer a wide variety of services and trading pairs, which may be used to facilitate money laundering, although this is typically a minor subset of legitimate activity. Although these exchanges are often unable to differentiate between illicit transactions committed by trafficked persons and fraud committed by criminal traffickers, they do possess KYC documents and can conduct additional diligence as needed, which may be useful to law enforcement. They also typically maintain relationships with one or more on-chain analytics vendors, enabling the detection of transactions involving addresses that have been flagged as relating to THB, CSAM, or other scams.

Coordinating with Centralized Stablecoin Issuers

Centralized stablecoin issuers - including the two largest, Tether and Circle - have the ability to freeze wallets by halting withdrawals from a wallet through the use of the issuing smart contract. As the most widely traded and utilized type of VA, stablecoins have also become the preferred asset for certain criminal typologies. Their high liquidity and a stable value, which mimic the traits of USD, make dollar-backed stablecoins more advantageous to criminals in the same way that the majority of criminal financial activity involves USD as opposed to other less liquid currencies. Criminals desire stores of value that can also be easily converted back to fiat currencies or used to purchase goods and services across borders, and stablecoins serve this purpose well for legal and illicit activities.

There are several types of stablecoin models, but only centralized issuers have the technical capability to freeze stablecoins in the secondary market. This is typically done upon the request of law enforcement, without necessarily requiring a court order. The ability to halt withdrawals from wallets has been used to freeze VA wallets listed on the SDN List by the U.S: Treasury's Office of Foreign Assets Control (OFAC), The National Bureau for Counter Terror Financing of Israel (NBCTF), and the UK's Office of Foreign Sanctions Implementation (OFSI). As of 15 September 2025, Stablecoin issuer Tether has frozen more than $3.2 billion in relation to law enforcement investigations.[109] The ability of stablecoin issuers to freeze VA wallets in response to international law enforcement requests is a powerful tool for public authorities. There are, however, certain limitations. Stablecoins are fungible and current blockchain technology only allows for the entire balance on a wallet to be frozen and not partial amounts. This means that if stablecoins have been sufficiently laundered across different

service wallets that contained previous balances unrelated to a crime, it may no longer be feasible for a stablecoin issuer to freeze the funds without incurring significant legal and financial risks. If only a small portion of a wallet's activity or balance can be traced to illicit activity, the counterparty risk may be too great for a stablecoin issuer to take action. In some instances, blockchain analysis may also label a wallet as being owned by a service. In such instances, where the identity of a service is known, law enforcement is incentivized to try to obtain information from the service about the criminal behaviour and the operator of the account being used for illicit purposes.

The closer the collaboration between law-enforcement agencies and stablecoin issuers, the quicker that VA wallets on the secondary market can be frozen, preventing criminals from moving the funds to where they can be laundered using untraceable means or where a freeze cannot be implemented, or converted into a VA that is not freezable – which is the vast majority of non-stablecoin VAs. Although the direct sharing of information and requests for action by stablecoin issuers is a more straightforward process than the indirect sharing of information derived from VASPs sharing suspicious activity reports with FIUs, which in turn provide such reports to law enforcement, law enforcement agencies and stablecoin issuers must still liaise and negotiate procedures for information sharing. This can be further complicated because stablecoin issuers do not have a presence in the same country as all law enforcement agencies. Stablecoin issuers may therefore elect to freeze wallets for international law enforcement either based on the service of legal process often through the use of MLATS, or on a voluntary basis.

Following investigations by stablecoin issuer Tether, leading crypto exchange OKX, blockchain forensics company Chainalysis, and the U.S. Department of Justice, Tether was able to voluntarily freeze approximately $225 million USDT that was being held in secondary market, self-custodied wallets linked to a money laundering network associated with a scam compound in Southeast Asia responsible for cyber scams on a massive scale. The joint investigation was conducted using tools from Chainalysis, and the action represents the largest ever freeze of USDT. Tether, OKX, and Chainalysis conducted a months-long investigation, which led to the companies proactively alerting law enforcement to the location of illicit funds. This prompted the United States Secret Service to request a freeze from Tether that was voluntarily executed by the company, as Tether is not a US-based company. In June 2025, Tether collaborated with the U.S. Department of Justice to burn the frozen assets and voluntarily reissue these assets to wallets controlled by the U.S. Department of Justice.[110/111] These proactive measures are an example of how the private sector can collaborate with global law enforcement agencies to more effectively deter illicit activity.

In addition to freezing funds, stablecoin issuers can also delete or "burn" a balance on a given VA wallet associated with their token. Stablecoin issuers can therefore burn frozen funds held in an illicit wallet and reissue these funds to the victim or a government agency. For example, Tether has completed such a process to assist in the re-issuance of $1 billion of funds related to crime[112]. Tether has seen a large increase in requests for token re-issuances, and has already processed 200 separate re-issuances in 2025. This ability to reissue funds that were illicitly gained is a strong deterrent to the criminal use of stablecoins, a great benefit to victims and governments alike, and may help to increase the proportion of criminal proceeds that are ultimately recovered.

Conclusion

This guidance paper, designed with six investigation steps, aims to highlight how criminals are exploiting digital technologies and digital financial tools in committing trafficking crimes and to show how law enforcement and other stakeholders can collaborate to more effectively redress the specific harms of trafficking in human beings in cyber-scam operations and child sexual exploitation, particularly where these crime typologies involve virtual assets.

The faceless, borderless nature of both social media platforms and VA exchanges has given savvy cyber criminals an asymmetric advantage over law enforcement that allows criminals to communicate and move value across borders with few restrictions, whereas law enforcement agencies must abide by strict jurisdictional limitations. This advantage can be mitigated, however, through effective collaboration between public and private stakeholders. The traceability of VAs and the freezability of stablecoins in the secondary market, in collaboration with LEAs around the world, highlights both the power and potential of such partnerships to enhance investigative results. There are, however, several areas where this collaboration could be strengthened.

1 The first is the level of coordination related to the ability of relevant stakeholders to share high quality data. With respect to coordination between LEAs and VASPs, when tracing illicit funds, whether funds have been traced to a VASP or have been converted to stablecoins and moved to private wallets, the most common reason that funds cannot be frozen is that too much time has passed since the initial money laundering transaction, allowing funds to be further laundered or mixed through a variety of methods that could render them untraceable. To minimize this risk, LEA should be proactive in knowing how to handle investigations related to VAs and stablecoins. This includes having knowledge of VAs, understanding how to use blockchain forensic tools, being aware of and able to contact large VASPs and stablecoin issuers that often work with LEA, and knowing what types of information these entities will require when responding to requests to freeze funds, whether based on a Mareva injunction or on a voluntary basis. Training should be collaborative between VASPs, blockchain tracing companies, and criminal justice agencies and as well between different LEAs. Furthermore, since there may be a range of law-enforcement agencies within each domestic jurisdiction, it may be helpful to centralize coordination with VASPs at the national level for smaller countries, and to have single points of contact within larger domestic LEAs that regularly collaborate with VASPs. These points of contact could be used to receive intelligence and proactively alert other VASPs regarding addresses tied to illicit flows.

2 The second area relates to better understanding trends in THB and CSE, so that red flag indicators can be detected and reported to law enforcement where appropriate. Private sector obligated entities, as well as social media companies, should take measures to familiarize themselves with the criminal typologies for which their platforms or services may be vulnerable (Step 2), as well as the corresponding red flags (Step 3). This can be facilitated with public private partnerships or other forms of collaboration (Step 4).

3 The third area relates to preventative education. While the aforementioned improvement of knowledge sharing between the private sector and law-enforcement agencies will help with detecting and addressing criminality, this recommendation pertains to educating the public with the aim of lowering their susceptibility to victimization. For example, initiatives such as "Know2Protect" work to educate children and their parents about the risks of CSAM and have a proven track record.[113] A similar program could be set up to educate segments of the public at risk for so-called "pig butchering," fake investments, or other types of financial scams. As some of the initial touch-points in these complex schemes, both banks and social media companies are well-positioned to make similar headway in this area with regards to awareness and education.

4 Finally, the fourth area is to leverage all available sources of information to identify as many victims as possible. This will maximize the ability for VASPs to be contacted in order to freeze funds held in VASP custody. Additionally, this will be helpful to stablecoin issuers as they investigate requests from law enforcement to freeze wallets and make a risk determination on whether a wallet can be frozen.

While digital technologies have expanded the scope and complexity of transnational crime, including THB and the production of CSAM, there are also new ways for law enforcement to fight back through collaboration with both public and private sector stakeholders. This report was written to spread awareness of the new ways that VAs and related technologies can be used to combat THB and the production of CSAM. May it serve to reduce these crimes and increase safety across the OSCE region.

Investigation Steps

STEP 1 Understanding Virtual Assets

In any criminal investigation involving virtual assets (VAs), the first step is to understand which assets are being used. Some VAs are more traceable than others, and it is important for LE to understand how these assets are transferred and where they can be stored.

Bitcoin (BTC), Ethereum (ETH), & Other Tokens
Most Virtual Asset (VA) transactions can be traced using public "scanner" websites such as https://etherscan.io or https://tronscan.org/#/ to reveal flow of funds (e.g., self-custody wallet vs. VA exchange platform). LE may only intercept funds via exchange platforms

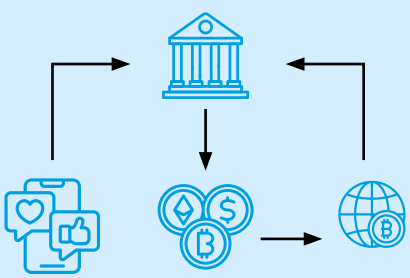
Stablecoins (USDT, USDC, etc.)
Unlike other VAs, fiat-backed stablecoins may be frozen and/or re-issued by the centralized issuer (e.g. Tether for USDT, Circle for USDC). While technically possible, issuers may have divergent legal requirements with regards to when and how they will freeze funds. These entities should be contacted for more information regarding their requirements for collaborating with law enforcement.

STEP 2 Understanding Criminal Modus Operandi (THB and Other Crimes)

The private sector must be aware of the indicators for THB or other crimes that they may be exposed to, so that monitoring and mitigation can be implemented, and law enforcement contacted when necessary. Utilizing a tiered system of both "red" and "yellow" flag indicators may help compliance officers with investigating transactions which deviate moderately from expected activity, but do not yet warrant reporting to law enforcement authorities.

Traffickers may use fake social media accounts to recruit victims for a variety of purposes:

- THB (Forced labour/fake job ads)
- THB (Sexual exploitation)
- Child sexual abuse/exploitation
- Financial Victims (Romance scams, e.g. so called "Pig Butchering")



Financial Victims may be persuaded to transfer funds from their bank accounts to VA trading platforms, to purchase VAs: Once victim funds have been converted into VAs, they may be rapidly transferred across services in different jurisdictions, to obscure their illicit origin. Funds may flow through a variety of services before reaching their final destination.

STEP 3 Red and Yellow Flag Indicators

Digital technologies enable organized crime groups to perpetrate increasingly sophisticated scams and frauds. They typically involve social media, may utilize a variety of crypto asset service providers or other financial institutions, and can span across a large number of jurisdictions.

THB for Forced Criminality
- Overly promising job advertisements, (e.g. work abroad with no experience)
- Mandatory on-site living; limited freedoms
- Presence of weapons, other coercion

Child Sexual Exploitation
- Recurring VA transactions to same group of addresses
- Frequent small value transactions, or purchases from sites linked to adult services
- VA transfers to mixers or CSAM-labelled addresses

Financial Victims
- Contact initiated on social media, but quick to switch to text messaging
- Initiates discussion of investment opportunities
- Introduces victim to 3rd party trading platform

STEP 4 Identifying Partners

Criminal financial investigations involving VAs may draw in a range of stakeholders from both the public and private sectors, and across multiple jurisdictions. It is important to understand which information can be provided, and by whom.

Public Sector
- National FIUs (Suspicious activity reports)
- Other domestic & foreign Law Enforcement
- Local LE Contact for crypto asset requests

Private Sector
- Global Social Media Companies (personal data & records)
- Financial Institutions (transaction activity & personal data)
- VA Exchanges (transaction activity & personal data)
- Centralized Stablecoin Issuers (Freeze & Re-issuance)

Virtual Asset Service Providers
Groups of stakeholders may already be collaborating to address specific problems in certain jurisdictions, via Public Private Partnerships (PPP). The Europol Financial Intelligence PPP (EFIPPP) in Europe, and the Illicit Virtual Asset Notification (IVAN) PPP are two examples of collaborative bodies that provide valuable insights and support to its members.

STEP 5 Gathering Evidence

Law enforcement may gather evidence from a variety of private sector stakeholders in multiple jurisdictions, who may also have divergent legal requirements with regards to the sharing of information

Social Media
- Chat histories
- Associate networks

Traditional Banks
- Transaction histories
- Personal account data

Virtual Asset Service Providers
- Transaction histories
- Personal account data

Blockchain Analytics Service Providers
Chainalysis & Elliptic enable both public and private stakeholders to track illicit funds

Chainalysis

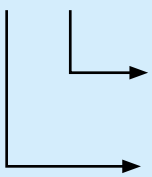
ELLIPTIC

STEP 6 Recovering Assets

Once illicit funds have been traced to a VA deposit address or service provider, law enforcement may collaborate with VA exchanges or centralized stablecoin issuers.

Collaborating with Virtual Asset Exchanges
Virtual Asset Exchanges may have personal data associated with crime-linked accounts, and may be able to block access to illicit funds that have been deposited to their platform and not yet transferred out. Most large exchanges have teams dedicated to law enforcement collaboration.

Collaborating with Centralized Stablecoin Issuers
Centralized stablecoin issuers may be retain the ability to freeze ("blacklist") or re-issue funds upon the request of law enforcement.



Collaborating with Banks
Most traditional financial institutions will require that LE produce a Mareva injunction before they will take action to freeze funds

Requesting an Asset Freeze
Upon the request of LE, stablecoin issuers may temporarily (or permanently) block funds

Requesting an Asset Re-issuance
LE may also request that frozen funds be "re-issued", in order to compensate victims

References

1 https://www.investopedia.com/terms/b/blockchain.asp.
2 https://www.21analytics.ch/glossary/crypto-asset-service-provider-casp/.
3 https://www.britannica.com/technology/darknet-Internet?.
4 https://www.coinbase.com/learn/crypto-basics/what-is-defi.
5 https://www.fincen.gov/resources/international/egmont-group-financial-intelligence-units?.
6 https://www.investopedia.com/terms/f/fiatmoney.asp.
7 https://definitions.uslegal.com/l/law-enforcement-agency/.
8 https://www.dwf-labs.com/news/crypto-otc-trading-meaning-benefits-and-comparison-with-traditional-finance?
9 https://www.investopedia.com/terms/p/ptop.asp?.
10 https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html?.
11 https://www.techopedia.com/definition/32499/smart-contract?.
12 https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-tor?.
13 https://www.techopedia.com/definition/cryptocurrency-wallet?.
14 An ecosystem approach to Web3.0: a systematic review and research agenda | Journal of Electronic Business & Digital Economics | Emerald Publishing.
15 https://www.osce.org/cthb/438527
16 Chainalysis Crypto Crime Report 2025 - https://go.chainalysis.com/2025-Crypto-Crime-Report.html
17 Crypto and Human Trafficking: 2026 Crypto Crime Report
18 IWF 2024: Commercial Websites Hosting Child Sexual Abuse Imagery
19 EU-SOCTA-2025.pdf
20 https://www.osce.org/oceea/587475
21 “Satoshi Nakamoto”, Bitcoin: A Peer-to-Peer Electronic Cash System” (2008)
22 Nathaniel Popper, “Digital Gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money” (Harper Collins, 2016)
23 Chainalysis Crypto Crime Report 2025, page 6 available at The 2025 Crypto Crime Report
24 Office of Public Affairs | Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes | United States Department of Justice
25 See The 2025 Crypto Crime Report, p.6
26 These are Algorand, Aptos, Arbitrum, Avalanche, Base, Celo, Ethereum, Hedera, Linea, NEAR, Noble, OP Mainnet, Polkadot, Polygon PoS, Solana, Stellar, Sui, Unichain, and ZKsync
27 https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-FATF-Report-G20-So-Called- Stablecoins.pdf
28 How does a booming crypto market affect child sexual abuse material?
29 https://cointelegraph.com/news/eu-crypto-ban-anonymous-privacy-tokens-2027
30 https://www.esrb.europa.eu/pub/pdf/reports/esrb.cryptoassetsanddecentralisedfinance202305~9792140acd.en.pdf
31 https://www.triple-a.io/cryptocurrency-ownership-data/cryptocurrency-ownership-data
32 Majority of APAC Consumers Prefer Remittance Services to Be Offered in a Super App - Fintech Singapore
33 The FATF Nine Special Recommendations (SRs) and Interpretative Note (IN)
34 FATF urges stronger global action to address Illicit Finance Risks in Virtual Assets
35 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, New York, 15 November 2000
36 DIRECTIVE (EU) 2024/1712 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims
37 Child Sexual Abuse Material vs Child Porn: What’s The Difference?
38 Alex Motshwanetsi Mathole, “Coverage of Modern Slavery and Human Trafficking in National Risk Assessments within Sub-Saharan Africa,” UNU-CPR Research Report (New York: United Nations University, 2023).
39 See: National_Risk_Assessment_of_Money_Laundering_and_Terrorist_Financing_2025_FINAL.pdf p. 26
40 OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, Policy Responses to Technology-Facilitated Trafficking in Human Beings: Analysis of Current Approaches and Considerations for Moving Forward (Vienna, March 2022)
41 https://polarisproject.org/human-trafficking-and-social-media/
42 https://www.trmlabs.com/post/unmasking-pig-butchering-scams-the-4-billion-crypto-scheme-preying-on-vulnerable-investors
43 See: A "wicked problem" - Seeking human rights-based solutions to trafficking into cyber-scam operations in South-East Asia | OHCHR; INTERPOL Crime Trend Update - Human trafficking-fueled scam centres (7).pdf
44 https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf
45 https://therecord.media/myanmar-pig-butchering-scams-cryptocurrency-payments-traced
46 In May 2025, a joint statement by UN experts noted that “hundreds of thousands of people of various nationalities are trapped and forced to carry out online fraud”. UN Special Procedures, UN experts urge immediate human rights-based action to tackle forced criminality in South-East Asia scam centres, 21 May 2025. See also INTERPOL, Crime Trend Update: Human Trafficking Fueled Crime Centres, June 2025. See also OHCHR,”A Wicked Problem” Seeking Human Rights-Based Solutions to Trafficking into Cyber Scam Operations in South-East Asia, February 2026
47 Global Anti-Scam Alliance, Global State of Scams, 2025 Report
48 See OHCHR, Corruption and Human Rights: a practical guide, 2025
49 https://www.iwf.org.uk/news-media/news/websites-offering-cryptocurrency-payment-for-child-sexual-abuse-images-doubling-every-year/
50 Crypto and Human Trafficking: 2026 Crypto Crime Report
51 https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child
https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/
https://go.chainalysis.com/Welcome-to-Video-case-study.html
https://www.chainalysis.com/blog/chainalysis-doj-welcome-to-video-shutdown/
52 https://www.justice.gov/usao-dc/pr/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child
https://www.forbes.com/sites/kellyphillipserb/2020/03/13/dark-deja-vu-irs-announces-charges-in-takedown-of-multi-million-dollar-child-exploitation-website-funded-by-bitcoin/?sh=34cd1b4628ae
53 https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf
54 Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users | Europol
55 (content from word doc Fintrac Case study provided by Tarana)
56 https://www.trmlabs.com/resources/blog/the-evolving-csam-landscape-vendors-increasingly-leveraging-ai-as-they-return-to-the-dark-web
57 https://www.chainalysis.com/blog/csam-cryptocurrency-monero-instant-exchangers-2024/
58 https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

59 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion
60 https://www.iwf.org.uk/about-us/why-we-exist/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery
61 iwf-ai-csam-report_update-public-jul24v13.pdf
62 https://www.rusi.org/explore-our-research/publications/commentary/global-anti-financial-crime-system-broken
63 https://www.osce.org/sites/default/files/f/documents/5/8/121125.pdf
64 https://www.moneylaundering.com/news/italys-efforts-against-defensive-strs-paying-off-albeit-slowly/
65 https://fintrac-canafe.canada.ca/intel/operation/exploitation-eng.pdf
66 https://fintrac-canafe.canada.ca/intel/operation/exploitation-eng.pdf
67 https://www.acamstoday.org/dr-kari-johnstone-and-tarana-baghirova-understanding-the-evolving-landscape-of-human-trafficking/
68 For example, see: https://www.humanity-consultancy.com/updates/the-horrible-5-month-life-in-scamming-compounds
69 For example, see: https://www.humanity-consultancy.com/updates/the-horrible-5-month-life-in-scamming-compounds
70 For example, see: https://www.humanity-consultancy.com/updates/swimming-across-the-moei-river-ayrans-journey-from-trafficking-to-triumph
71 For example, see: https://www.humanity-consultancy.com/updates/from-bypassing-immigration-at-thailands-pattaya-airport-to-trafficking-hell-in-scam-industry-mahmuds-story
72 For example, see: https://www.humanity-consultancy.com/updates/from-bypassing-immigration-at-thailands-pattaya-airport-to-trafficking-hell-in-scam-industry-mahmuds-story
73 For example, see: https://www.humanity-consultancy.com/updates/swimming-across-the-moei-river-ayrans-journey-from-trafficking-to-triumph
74 For example, see: https://www.humanity-consultancy.com/updates/swimming-across-the-moei-river-ayrans-journey-from-trafficking-to-triumph
75 Exposing Money Laundering Techniques in Pig Butchering Scams | ACAMS
76 (LE definition) - https://bjs.ojp.gov/topics/law-enforcement#:~:text=Law%20enforcement%20describes%20the%20agencies,individuals%20suspected%20of%20criminal%20offenses.
77 (EUROPOL mission) - https://www.europol.europa.eu/about-europol
78 https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/
79 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.inline.pdf
80 STRATEGIC ANALYSIS REPORT - THB.pdf
81 Intelligence-Factsheet.pdf
82 Publications of the Money Laundering Reporting Office Switzerland (MROS) First anti-trafficking guide for financial institutions launched by OSCE and Swiss Money Laundering Reporting Office | OSCE
83 Our Intelligence Services, STOP THE TRAFFIK
84 https://childrescuecoalition.org/about-us/
85 https://followmoneyfightslavery.org/
86 https://followmoneyfightslavery.org/testimonials/
87 EFIPPP_Practical_Guide.pdf
88 The European Banks Alliance in May 2017 launched an innovative Toolkit for tackling human trafficking. https://www.trust.org/banks-alliance/
89 https://fintrac-canafe.canada.ca/emplo/project-projet/psr-eng.pdf
90 https://www.icmec.org/financial-coalitions/
91 https://ecpat.se/wp-content/uploads/2020/12/Project-Indicators-EN.pdf
92 Binance.US joins U.S. law enforcement-led initiative to share actionable intel on emerging threats
93 Announcing the Tech Against Scams Coalition
94 https://efippp.eu/
95 FIU Luxembourg, Rapport annuel 2021 et 2022, Rapport d'activité de la Cellule de renseignement financier, July 2023, 56 and 57.
96 https://amlcenter.lt/en/
97 https://fid.gov.lv/en/roles-and-responsibilities/public-private-partnership
98 European Banking Federation, EBF Response to Public Consultation on Guidance on the Rules Applicable to the Use of Public-Private Partnerships in The Framework of Preventing and Fighting Money Laundering and Terrorist Financing, 2021.
99 FIU Latvia, Regulation on the Operation of the Cooperation Coordination Group of the Financial Intelligence Unit, August 2019.
100 FIU The Netherlands, Annual Review, 2019. See for more information and infographic: https://www.fiu-nederland.nl/en/home/partnerships/
101 https://www.fec-partners.nl/over-fec/english/
102 The FEC is a public-public body, see https://www.fec-partners.nl/over-fec/english/
103 https://home-affairs.ec.europa.eu/news/european-ports-alliance-fight-drug-trafficking-and-organised-crime-2024-01-24_en
104 https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en
105 EDPB letter to the European Parliament, the Council and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations, March 2023.
106 https://www.osce.org/files/f/documents/2/1/587475.pdf
107 https://www.dhs.gov/know2protect/about
108 https://www.dhs.gov/sites/default/files/2025-04/25_0422_k2p_2024-year-review.pdf
109 https://tether.io/news/tether-supports-canadian-law-enforcement-in-recovery-of-460000-usdt-from-investment-fraud-scheme/
110 https://tether.io/news/following-investigations-by-tether-okx-and-the-us-department-of-justice-tether-voluntarily-freezes-225m-in-stolen-usdt-linked-to-international-crime-syndicate/
111 https://www.justice.gov/usao-dc/media/1403996/dl?inline
112 https://www.justice.gov/opa/pr/cyber-scam-organization-disrupted-through-seizure-nearly-9m-crypto
113 https://www.dhs.gov/sites/default/files/2025-04/25_0422_k2p_2024-year-review.pdf

The Organization for Security and Co-operation in Europe works for stability, prosperity and democracy in 57 States through political dialogue about shared values and through practical work that makes a lasting difference.

OSCE Organization for Security and Co-operation in Europe