BASEL INSTITUTE ON GOVERNANCE

EUROPOL

INTERPOL

Combating virtual assets-based money laundering and crypto-enabled crime

2021 Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies

These seven Recommendations emerge from the 5th Global Conference on Criminal Finances and Cryptocurrencies, held virtually on 7-8 December 2021. The annual conference is organised by the Working Group on Criminal Finances and Cryptocurrencies, a tripartite initiative of the Basel Institute on Governance, INTERPOL and Europol that dates back to 2014 and was formally established in 2016.

The Recommendations are intended to guide law enforcement, judicial authorities, regulators and the private sector in broad approaches that are necessary to protect citizens and the global economy from the risks of abuse of cryptocurrencies and other virtual assets.

Introduction

A fast-evolving sector: fresh opportunities, new threats

The rapid evolution of the virtual assets industry, including its possibilities to launder money and commit crimes in the cyber and physical worlds, demands a rapid response from government policymakers, regulatory bodies, judicial authorities, law enforcement and the private sector. There are two main reasons why this is important.

First, it is essential to combat new threats as they arise – or if possible, anticipate them.

A current example is **Decentralised Finance (DeFi)** services, an emerging area of concern for virtual assets-based money laundering due to their apparently decentralised, autonomous and anonymous nature.

Likewise, markets around **non-fungible tokens (NFTs)**, gaming and the **metaverse** call for greater attention by law enforcement, regulators, the private sector and developers of cyber forensics tools and techniques.

Second, the nature of virtual assets and blockchain technologies opens up fresh opportunities to combat money laundering.

Organised crime groups and others that operate **darknet marketplaces**, launch **ransomware attacks** or carry out **fraud schemes** are increasingly using cryptocurrencies to make and receive payments and to launder their illicit funds.

This gives law enforcement an advantage, because cryptocurrency transactions are recorded permanently in a publicly accesible ledger – the blockchain. **The information cannot be altered or falsified**, unlike most monetary transactions in the physical world. Financial investigations can trace funds through the blockchain and gather evidence years after a crime has taken place. Also enshrined in the blockchain are errors made by criminals, which can help to reveal a suspect's identity or wider network.

Recommendations

1. International cooperation

Make existing channels of international cooperation stronger, faster and more proactive, to counter the lightning-fast and hyperglobal nature of virtual assets. This includes efforts to strengthen both formal and informal cooperation between law enforcement agencies

and judicial authorities, as well as between law enforcement and Virtual Asset Service Providers (VASPs) based in other jurisdictions.

The virtual assets industry is hyperglobal, and criminals can operate crypto-enabled crime schemes or launder illicit funds on the other side of the world just as easily as they can at home. Transactions take place at lightning speed and are often irreversible.

Law enforcement agencies can and should maximise the use of **existing channels of both informal and formal cooperation to exchange information** that can help to identify, investigate and prosecute those using virtual assets for illicit purposes. This includes the global cooperation mechanisms provided by INTERPOL and Europol, such as the SIENA channel and the network of National Central Bureaus (NCBs), as well as bilateral and multilateral channels with VASPs based in different jurisdictions (see Recommendation 3). For example, in cases of serious and organised crimes, it should be standard practice to check names, telephone numbers and cryptocurrency addresses with Europol to cross-check with other investigations.

Speeding up information exchange and the **sending, receiving and actioning of judicial requests** should be a priority, particularly where funds need to be frozen before they are dissipated or disappear. The hyper-speed nature of virtual assets means that all and any efforts in this area will result in significantly improved outcomes for investigations, prosecutions and asset recovery.

When **resources (new techniques, best practices, new strategies) are developed** that could be useful for all law enforcement authorities, these should be **shared widely** to prevent duplication of work and ensure a consistent and harmonised response.

International cooperation should extend to developing standards and best practices in tackling virtual assets-based money laundering, as well as sharing emerging modi operandi and investigative techniques. Conferences, workshops and knowledge-sharing sessions are key to this effort, as well as to building the trust and relationships that are foundational for effective international cooperation.

2. Virtual asset recovery

Treat virtual assets like traditional assets – such as jewellery or artwork – to facilitate their freezing and confiscation. Easing the recovery of virtual assets helps not only to return stolen funds, but also to deter future crypto-enabled crimes and virtual assets-based money laundering.

Cryptocurrencies and other virtual assets should be regarded like any other assets in terms of implementing tried-and-testing asset

recovery best practice. Recognised strategies such as pre-seizure planning and public-private collaboration have been pivotal in many jurisdictions. Approaching crypto like a complex asset has enabled agencies to recover significant amounts of crypto assets and convert them into fiat currencies through exchanges or auctions.

However, some jurisdictions have not yet taken this best practice on board in their laws and procedures. As a result, they miss opportunities to **disrupt criminality, identify illicit financial flows and recover assets** for the benefit of victims and wider society.

As the quantity of illicit assets held in the form of cryptocurrencies grows, this failure to implement international best practice will be an increasing obstacle to countries' efforts to fight financial crime.

This is because asset recovery is not only about returning criminal proceeds to victims and governments, but about preventing and deterring corruption, organised crime and other illicit activity. **Recovering illicit assets raises the risk and cost of crime,** reduces the potential reward and helps ensure that crime does not pay.

All stakeholders should actively engage in **developing and applying emerging international best practices in virtual asset recovery.** This includes sharing knowledge on ways to freeze and seize virtual assets, to manage them effectively in order to retain their value while criminal proceedings are underway, to overcome issues of volatility, and to convert them into fiat currency following the confiscation order. A good example of this is the subgroup on virtual currencies within the Asset Recovery Office (ARO) platform hosted by the European Commission, in which Europol and EU AROs participate.

3. Public-private cooperation

Establish trust and effective mechanisms for public-private cooperation to address virtual assets-based money laundering, especially between law enforcement and VASPs. Cooperation can be bilateral, multilateral or through public-private partnerships, and should cover both operational and strategic information sharing.

Combating virtual assets-based money laundering is a major ongoing challenge and requires all stakeholders to pool their expertise, information and resources.

Cryptocurrency exchanges and other VASPs – like all financial institutions – have information and technical capabilities that can **support law enforcement investigations and asset recovery**, including tools for data analysis and live monitoring. They also have the ability to blacklist users, lock accounts and contact suspects to refund stolen funds. **Close cooperation**, including via joint investigations

where appropriate, can help law enforcement agencies to do more with fewer in-house resources.

Speed is another benefit of public-private cooperation. For example, transaction monitoring tools developed by exchanges can help them to identify transactions potentially linked to illegal activity. Leads can then be referred to the law enforcement agency, which can quickly send and receive the relevant information through formal legal channels. Custom follow-up is also possible in this scenario, instead of automated blocking or off-boarding by the exchange acting alone. In the case of high-priority incidents, exchanges can take immediate action.

Information-sharing at the strategic level – for example about hacking attempts, fraudulent activity, money laundering modi operandi, devices used, newly discovered trends, suspects and victims – can help exchanges and other VASPs to improve their defences and detection algorithms. This in turn means that law enforcement can better focus their investigations and contributes to prevention, awareness and capacity building on both sides. Collaboration on capacity building can also help specialist law enforcement units to stay at the cutting edge of developments in the virtual assets industry.

Both operational and strategic information sharing are facilitated where VASPs have **dedicated departments for cooperating with law enforcement** and other government bodies, including internationally. Contact details for such departments should be made available to all law enforcement authorities to facilitate subpoenas and requests from investigators to VASPs.

Law enforcement agencies need to be ***proactive about directly approaching VASPs*** and building mechanisms for cooperation and information sharing. Europol and INTERPOL can support these efforts by facilitating initial contacts. Stakeholders can also consider using **existing public-private partnerships** as a platform for exchanging information and building trust, such as the Europol Financial Intelligence Public Private Partnership (EFIPPP).

4. Harmonised regulation and its effective implementation

Ensure smart, harmonised regulation that draws on wide-ranging expertise and looks ahead to future challenges. It is essential that all national authorities implement international regulations effectively, to prevent money laundering activity simply moving to jurisdictions with weak and poorly enforced regulations.

Regulation of virtual assets is challenging because they do not easily fall into traditional categories of AML regulation such as e-money, securities or financial instruments. The nature of cryptocurrencies makes it difficult

to impose regulatory requirements on the asset itself. This makes crypto assets highly vulnerable to use for illicit purposes and money laundering.

There is a strong need for specific regulations in order to set the parameters for market participants and establish a framework for investigators to approach bad actors in the system. Standards need to be **harmonised internationally**, to prevent criminals from engaging in regulatory arbitrage – simply moving their operations to jurisdictions with weak and poorly enforced regulations on virtual assets-based money laundering.

All distributed ledger technology (DLT)-based services that have elements of centralisation should be **subject to anti-money laundering and counter financing of terrorism (AML/CFT) regulations** like any other reporting entities. Given the cross-border nature of crypto assets and increased use of privacy mechanisms to conceal the source of funds or wealth, VASPs will be expected to apply a risk-based approach in evaluating the appropriate due diligence for each customer, product, transaction and asset type. Additional effort may be required to bring **DeFi platforms under supervisory control**, relying on the presence of centralised features such as the ability of a natural person or legal entity to modify smart contract features over time.

Recent regulatory developments address some of the risks associated with the use of cryptocurrencies. However, competent authorities still need to **speed up implementation of international standards**, especially of the so-called travel rule, and address consumer protection and other regulatory risks.

A forward-looking approach is also needed to address challenges around the corner, such as arising from **NFTs, the metaverse and the gaming industry**. Competent authorities should closely monitor developments in this area, and consult widely with industry and law enforcement stakeholders to more fully understand the impacts of certain policies, which may be different to those one might expect in traditional financial markets.

5. Investigative techniques and technologies

Rapidly develop, adapt and evolve investigative technologies and techniques to keep up with the criminals. In this effort, it is helpful to leverage the innovation capacity of the private sector.

As a broad modus operandi, virtual assets-based money laundering is evolving fast. Law enforcement should recognise the potential for money laundering through new forms of cryptocurrencies and other virtual assets, such as NFTs, and develop procedures to address such use.

Traditional investigative techniques such as undercover investigations

and controlled delivery need to be **adapted to the current scenario**. Crypto tracing and other techniques such as tactical surveillance and analysis of transaction and tax information (financial investigation) should also be applied.

The **private sector** can be a powerful partner to law enforcement in developing and using new technologies for tracing funds held in cryptocurrencies. For example, blockchain analytics firms are responding to the challenges of tracing funds exchanged on decentralised platforms by innovating fast: new screening tools for technologies such as oracles, liquidity pools and smart contracts are already being developed.

VASPs also hold information that can help to develop new investigative techniques to address emerging technologies in the crypto sphere. **Training and joint workshops or conferences** can help to transfer this vital knowledge. Examples are those organised by the EFIPPP, the Europol Platform for Experts (EPE) and the Tripartite Working Group on Criminal Finances and Cryptocurrencies, as well as Europol's Virtual Currency Conference.

It is not only law enforcement that needs to adapt investigative techniques; **judicial authorities** also need to develop new strategies to address virtual assets-based money laundering.

6. Capacity building

Invest massively in capacity building, especially for those in law enforcement and the private sector in a position to detect virtual assets-based money laundering. Building capacity is not only about training existing staff, but about changing hiring practices to attract those already skilled in the cyber sphere.

The virtual assets industry is expanding and evolving at an incredible rate. Capacity building should be widespread, with a particular focus on:

- **Strengthening the capabilities of specialised law enforcement units** to address crypto-related threats. These units are well placed to transfer skills within their own agencies (see next point) through in-house capacity building and awareness-raising.

- **Accelerating the training of "front-line" staff in a position to detect crypto-enabled crimes.** In law enforcement, this means first responders and those involved in investigating serious organised crime, corruption and other financial crimes. In the private sector, AML compliance professionals in particular need to quickly upskill. Early detection aids investigation and the timely freezing of suspect funds before they can be dissipated or hidden.

- **Ensuring judicial authorities have the required knowledge** and

capabilities to act fast when subpoenas and judicial requests are needed.

- **Ensuring AML supervisors** correctly understand new business models, their associated risks and how to address them.

Building capacity is not only about training existing staff. Hiring practices should adapt. Both law enforcement and the private sector need to attract talented "digital natives'' with high levels of technical expertise. (See also Recommendation 7.)

7. Multidisciplinary approach, including through specialised law enforcement units

Combine the expertise of financial investigators, IT/forensics experts and cybercrime specialists to tackle cases of virtual assets-based money laundering and related crypto-enabled crimes. In a law enforcement context, this means increasing intra-agency cooperation between different units. Where feasible, specialist teams could also be established to lead complex cases and provide in-house support to other units.

A multidisciplinary approach is increasingly recognised as essential to tackling complex crimes, including those of a financial nature. In the crypto sphere, this is multiplied by the high level of **specialised expertise required in IT, cybercrime and financial investigation**.

Increasing numbers of law enforcement authorities have set up **multidisciplinary units** focused on crypto-enabled crimes. However, they remain small and insufficiently resourced when one considers the relative sizes of the physical and digital domains. This is true even now, and will be even more so in the future as the digital sphere grows.

Specialised units have the ability to move fast, conduct their own investigations and support investigations led by other law enforcement units. They can and do also cooperate efficiently with central government authorities as well as internationally. An **effective and integrated multidisciplinary approach** also requires the support of specialised judicial authorities.

Where resources do not exist for dedicated specialised units in law enforcement agencies, it is recommended to introduce measures to **increase intra-agency and inter-agency coordination**. These could include multidisciplinary working groups, task forces or joint investigation teams.