



Financial investigations of money
laundering involving Virtual Assets

Tirana, June 22



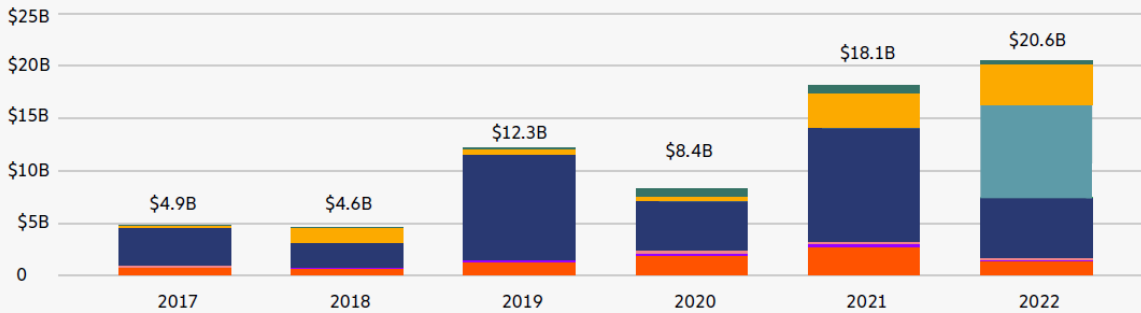
Outline

- VA-related trends
- Elements of effective framework to detect and investigate ML with use of VA
- UNODC work in this area
- Open discussion

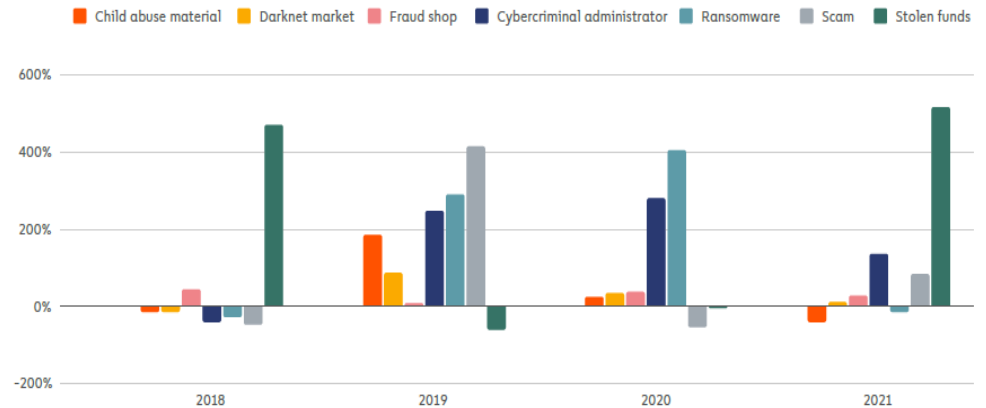
\$20 bln received by illicit addresses in 2022

Total cryptocurrency value received by illicit addresses, 2017 - 2022

■ Child abuse material
 ■ Ransomware
 ■ Stolen funds
 ■ Sanctions
 ■ Terrorism financing
■ Scam
 ■ Cybercriminal administrator
 ■ Fraud shop
 ■ Darknet market



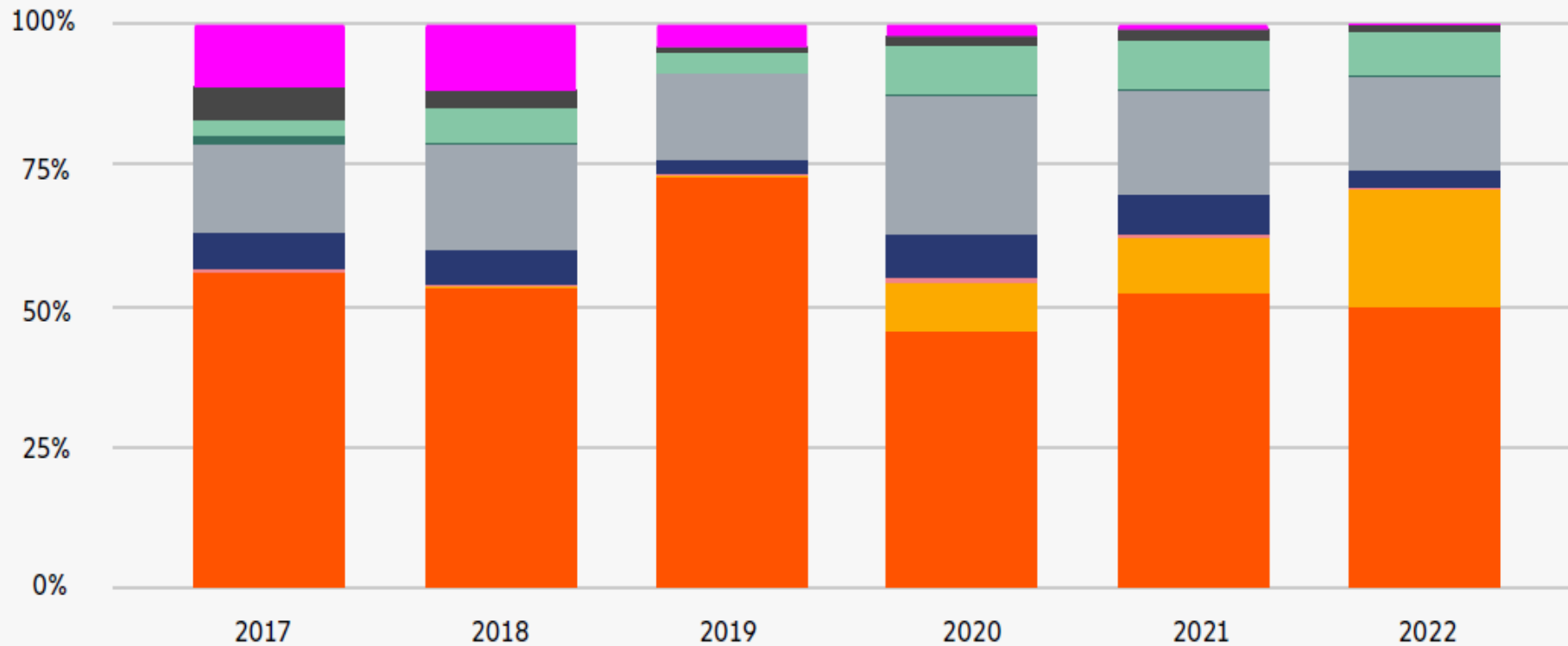
Year over year percent change in value received by crime type | 2018-2021





Destination of funds leaving illicit wallets, 2017–2022

- P2P exchange
- Other
- Mixing
- Mining
- High-risk jurisdictions
- High-risk exchange
- Gambling platform
- DeFi
- Centralized exchange



Darknet markets



DeepMarket Login Register Status order Escrow Support Blog About Us Messages 0 item(s) - \$0.00

Carding Money transfers Gift cards Money counterfeits Hacking Documents Electronics Other

ASIA

UnionPay & VISA. The fastest delivery in Asia


Category: Carding
Status: Online
Member since: Oct 2016
Sales: 13225
Rating:
Buyer protection: Yes

Buyer Protection

- Full Refund if you don't receive your order
- Full or Partial Refund, if the item is not as described

About Vendor

We are a team of professional carders from China. We ship prepaid cards worldwide, but if you live in Asia, you will receive your order in a few days.
We only use express delivery to get your order as soon as possible.
We will ship your order within 24 hours after purchase. After sending we will send you the tracking number.
All our cards are registered in the Visa and UnionPay network.
We give a guarantee on all our products.



APOLLON

Profile items:

- Home
- Items
- Orders
- My Profile
- My Feedback
- My Wishlist
- My Favorites
- Support

Deposited & Withdrawn BTC

Deposited & Withdrawn EUR

Deposited & Withdrawn LTC

Deposited & Withdrawn BCC

My Profile

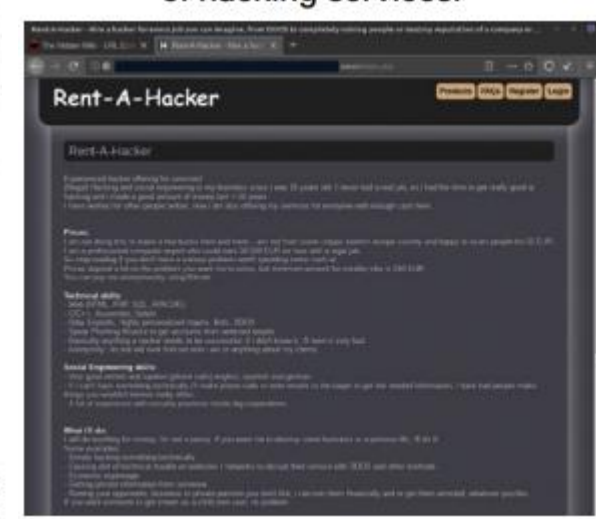
My Feedback

My Wishlist

My Favorites

Support

Counterfeit card service



Rent-A-Hacker

Professional hacker offering for yourself

Services:

- DDoS (Residential, Server)
- Phishing (Social, Email)
- Website Security Audit
- SQL Injection
- Web Application Penetration Testing

What I'll do:

- DDoS (Residential, Server)
- Phishing (Social, Email)
- Website Security Audit
- SQL Injection
- Web Application Penetration Testing

Compromised financial info



APOLLON

Profile items:

- Home
- Items
- Orders
- My Profile
- My Feedback
- My Wishlist
- My Favorites
- Support

Deposited & Withdrawn BTC

Deposited & Withdrawn EUR

Deposited & Withdrawn LTC

Deposited & Withdrawn BCC

My Profile

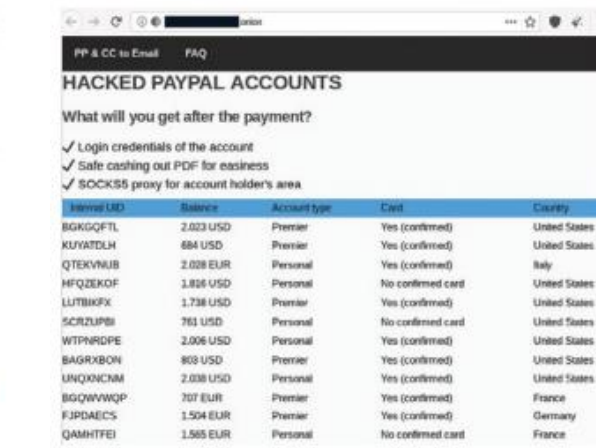
My Feedback

My Wishlist

My Favorites

Support

Hacking services



HACKED PAYPAL ACCOUNTS

What will you get after the payment?

- ✓ Login credentials of the account
- ✓ Safe cashing out PDF for easeless
- ✓ SOCKS5 proxy for account holder's area

Internal UID	Balance	Account type	Card	Country
BGKGQFTL	2.023 USD	Premier	Yes (confirmed)	United States
KUVATDLH	684 USD	Premier	Yes (confirmed)	United States
QTEKVNJB	2.028 EUR	Personal	Yes (confirmed)	Italy
HFQZKQF	1.816 USD	Personal	No confirmed card	United States
LUTBKFX	1.738 USD	Premier	Yes (confirmed)	United States
SCRZUPBI	761 USD	Personal	No confirmed card	United States
WTPNRDPE	2.006 USD	Personal	Yes (confirmed)	United States
BAGRXBON	808 USD	Premier	Yes (confirmed)	United States
UNQXNCNM	2.038 USD	Personal	Yes (confirmed)	United States
BGQVWQP	707 EUR	Premier	Yes (confirmed)	France
FJPDACES	1.504 EUR	Premier	Yes (confirmed)	Germany
QAMHTEI	1.565 EUR	Personal	No confirmed card	France

Illegal wildlife trade

*Shows vendor sending drugs from Singapore to anywhere in the world.
Drugs



Top 25 darknet markets and fraud shops by revenue, 2022



- Migration of vendors from Hydra to other markets
- DW Markets offering ML services – VA transfer and withdrawal



Trends in criminal use of crypto assets

- Use of Centralized Exchanges (CEX) in high-risk jurisdictions
- Gradual shift to Decentralized Exchanges (DEX) or Hybrid (CEX over DEX) – No KYC/AML
- Big CEXes are still popular (criminals also value credibility) – use of nested exchanges – No KYC/AML
- OTC brokers nested on exchanges
- Growth of underground ML services
- ML services offered directly by Darkweb marketplaces
- Use of anonymity-enhanced cryptocurrencies (AEC)

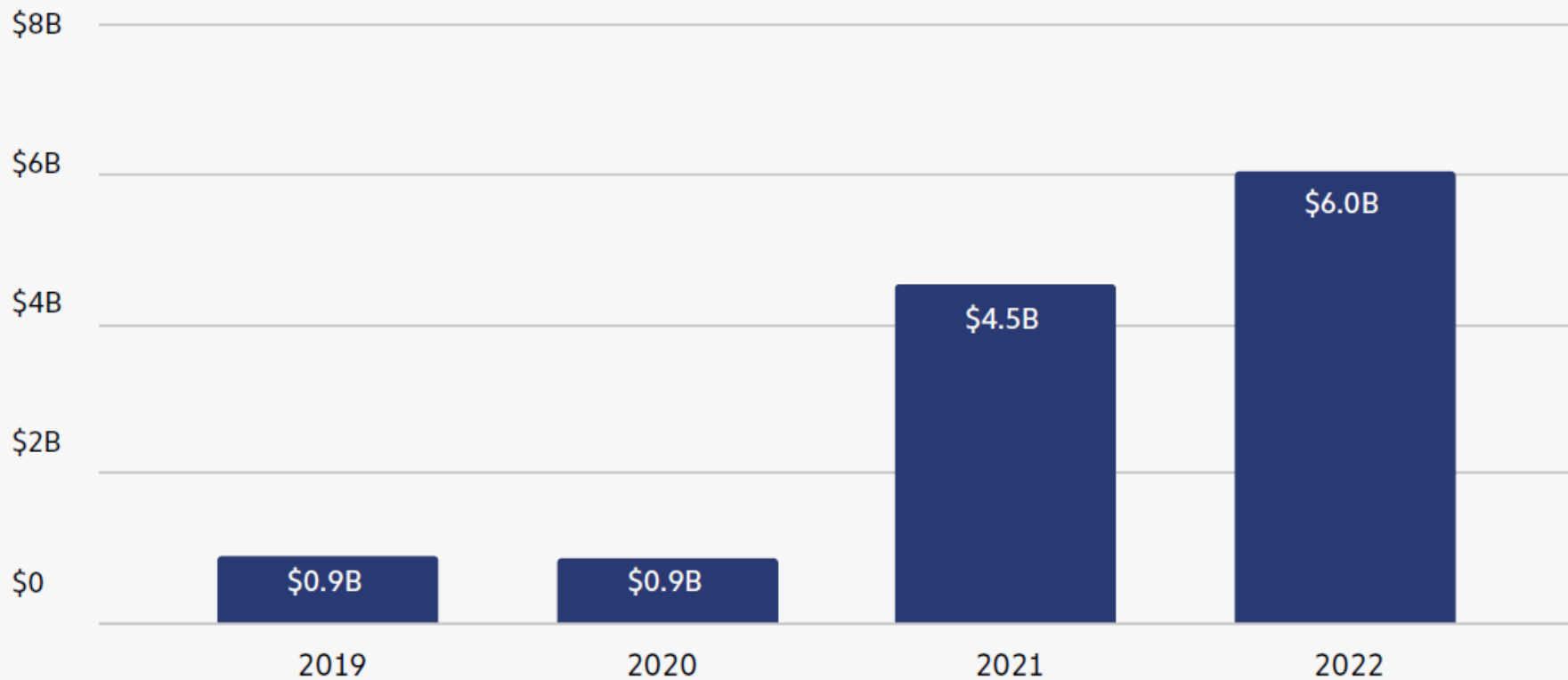


Trends in criminal use of crypto assets

- Use of DeFi, in particular smart contracts
- Deploying fictitious smart contracts to obfuscate transactions
- Exploiting largely unregulated NFT market for ML
- Use of the Bitcoin **Lightning network**: private channel is opened between counterparts to transfer cryptocurrency without creating a on-blockchain transaction for individual payments (thus no records of individual transactions – only the final settlement)



Total illicit value moving to suspected underground laundering services, 2019–2022



Layering and anonymisation methods – new trends



PML services

Money mules

Crypto ATM

Unregistered
VASPS



Chain
Hopping

Coin Joins

Enhanced

Mixers

Anonymity Coins

Lightning
Network

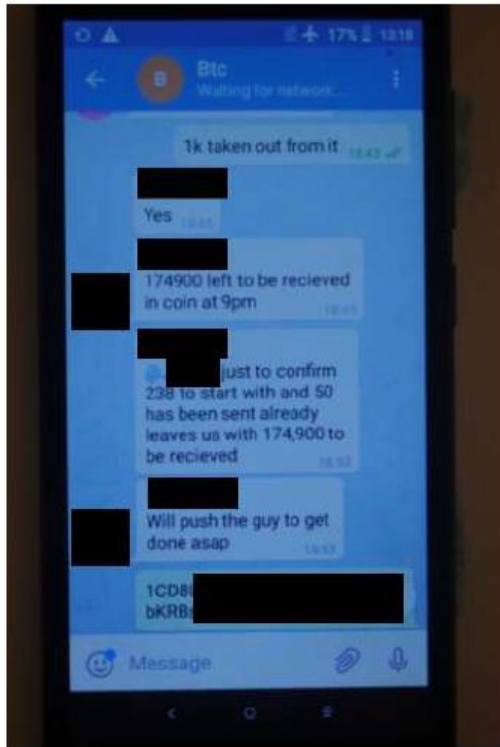
Non Custodial
Wallet

Non-compliant
exchanges

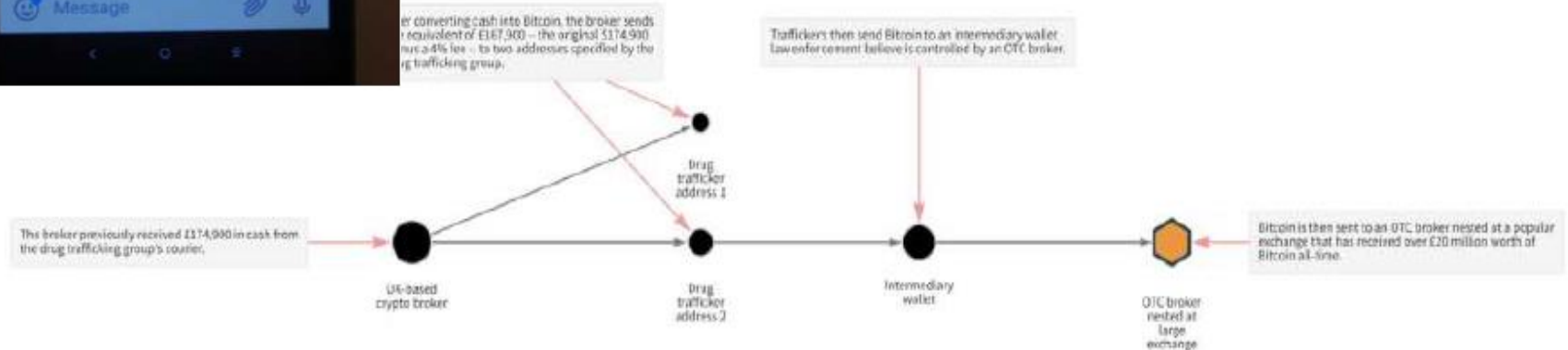
Crypto vouchers



Nested over-the-counter (OTC) services



- Drug proceeds in cash are delivered to broker
- The broker converts money in bitcoins and sends them to an address specified by the crime group;
- 4% transaction fee
- funds were ultimately sent to an OTC service nested at a popular cryptocurrency exchange;
- drug trafficking group laundered at least £1 million across several Bitcoin transactions using these methods





VA and money mules professional ML schemes

EUROPOL **Operation 2BaGoldMule**
Criminal Group QQAAZZ

COOPERATION

Operation led by: Portugal United States of America

with the support of:

Austria	Belgium	Bulgaria	Czech Republic	Germany
Latvia	Poland	Spain	Sweden	Italy
United Kingdom	Australia	Georgia	Switzerland	

Legend:
 ■ Countries involved in the operation
 // Countries with victims
 ● Main points where the criminals operated
 🚔 Arrests
 🏠 Money muling activities
 △ Shell companies

MODUS OPERANDI

- ### 1 STRUCTURE OF THE CRIMINAL GANG

Comprised of several layers of members from Latvia, Georgia, Bulgaria, Romania, and Belgium who supervised a network of money mules.

Criminals used sophisticated malware to steal money from victims' accounts
- ### 2 MONEY LAUNDERING

Money mules used both legitimate and fraudulent Polish and Bulgarian ID documents to open hundreds of bank accounts all over the world.

Money laundering services advertised on Russian-speaking online criminal forums

Bank accounts available to receive stolen funds

Additional bank accounts were opened in the name of these companies

Created and registered shell companies
- ### 3 REINVESTMENT

With the laundered money, criminals opened legitimate businesses in a number of other European countries.

EUROPOL www.europol.europa.eu



With all variety of scams, malwares and other predicate offending the financial schemes will have a lot of similarities.

Targeting illicit finances remain the most effective way to disrupt cyber-enabled crime.



Elements of an effective framework

- Understanding of existing risks and modus operandi of criminal and ML networks
- Access to various sources of financial and non-financial information (including technical data) that can support the financial investigation
- Bridging financial investigators and digital forensics labs
- Partnership with the private sector
- VASPs regulation and supervision, detection of underground VASPs
- Effective multiagency cooperation, JITs
- Mechanisms for rapid restraint and transaction postponement
- Effective formal and informal international cooperation mechanisms
- Selection of the best channel to request information from foreign VASP (directly, Egmont, Interpol)
- Use of new technologies for data analysis, OSINT, Machine Learning



Data required for investigation

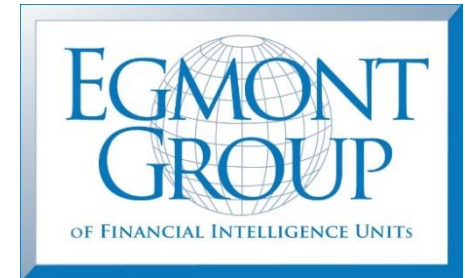
- VA addresses
- Account information
- Transaction details (including virtual currency transaction hash and information on the originator and the recipient)
- Relevant transaction history
- Available login information (including IP addresses)
- Mobile device information (such as device IMEI)
- Information obtained from analysis of the customer's public online profile and communications.
- Cryptocurrency wallets/addresses and associated blockchain records
- Various identification numbers including IMEI13, IMSI14 or SEID15 numbers as well as MAC addresses16
- Login behaviour and IP data
- Geolocation data
- Identification (e.g. authentication cookies) and information stored on devices
-



Information sharing and transaction restraints opportunities

Egmont Biennial Census – a resource tool to get information on:

- Data that can be provided by each FIU
- Lists of reporting entities
- Requesting powers
- Restraint/freezing powers (terms and modalities)
- Access to external databases



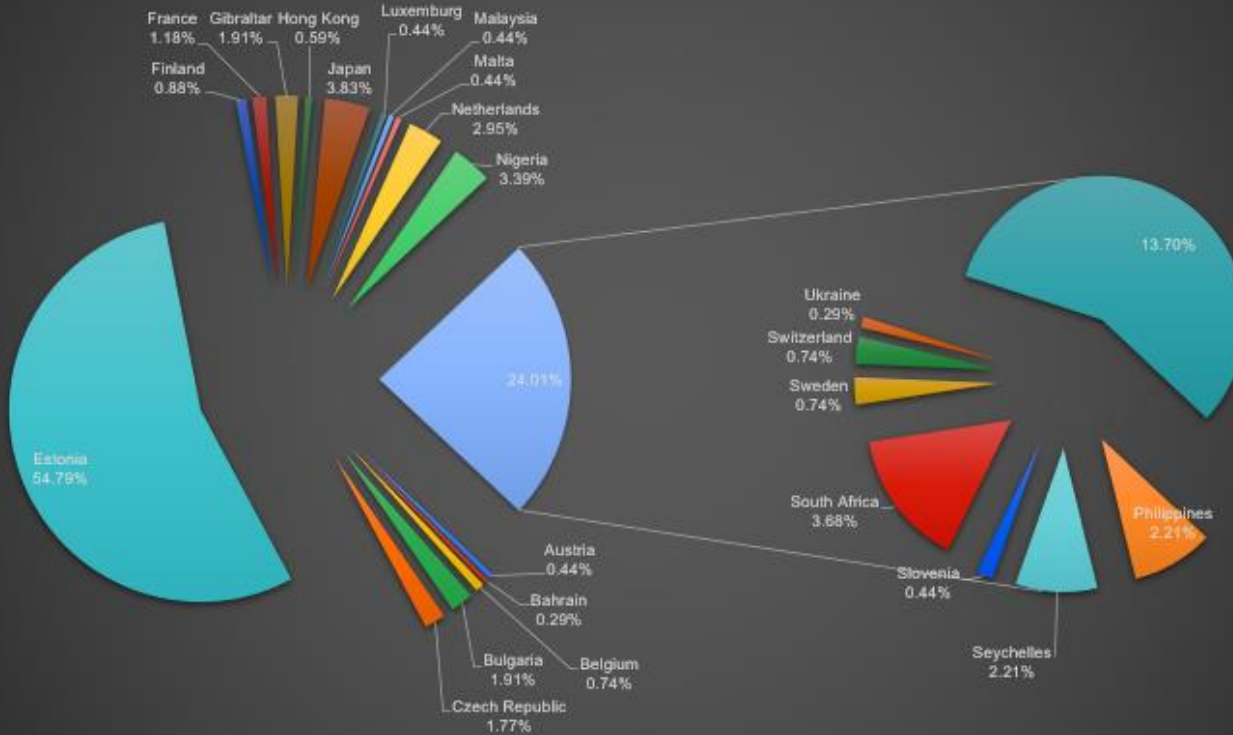
VASPs e-catalogue: more than 700 VASPs, will be updated, for official use only

- TOP VASPs
- Where registered, which information can be provided (incl. financial and technical data)
- Restraint opportunities
- Standard request form
- How to understand which VASP is used?



VASPs e-catalogue

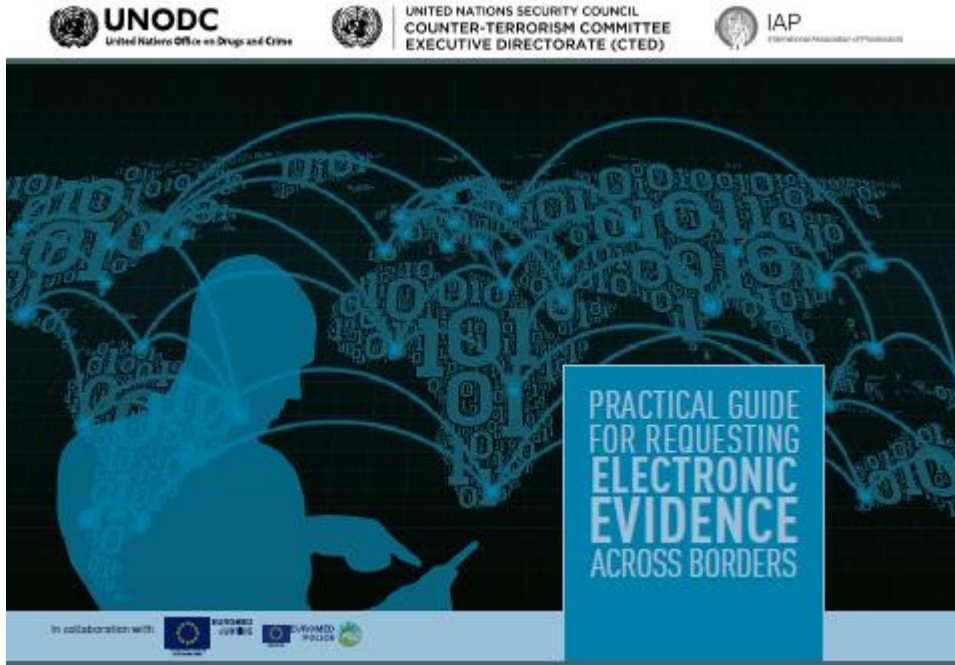
Distribution of Reported VASPs Globally (based on VASPs reported)



Country	VASP Name	Legal Entity	Address	Website	Registry
Austria			2000 Antwerpen		
Austria					commercial/official register
Austria					atenbank Suche FMA Österreich
Austria					atenbank Suche FMA Österreich
Austria					atenbank Suche FMA Österreich
Bahrain					tps://www.sijilat.bh/
Bahrain					ov.bh/licensing-directory/#register
Belgium					KBO
Belgium					KBO
Belgium					KBO
Belgium	CryptoWaas	MVP Automatic	Avenue Louise 231, 1050 Ixelles	http://www.cryptowaas.be	KBO
Belgium	Orillia	Orillia BVBA	Rivierstraat 6A, 9270 Laarne (Belgium)	www.orillia.be	KBO
Bulgaria	BellaChain	BellaChain OOD	seat and management address: Varna city, 9000, Odessos region, 4 Baruten Pogreb Str.	Bellachain.net	Търговски регистър и регистър на ЮЛНЦ NRA
Bulgaria	Bitcoin Solutions	Bitcoin Solutions EOOD	seat and management address: Sofia city, 56-58 Krump Popov Str.	https://crypto.bg/	Търговски регистър и регистър на ЮЛНЦ NRA
Bulgaria	Blockchain Tech	Blockchain Tech EOOD	seat and management address: Sofia city, 96 Aleksandar Stamboliyski Blvd., fl. 1, apt 29	https://cryptodesk.bg/ https://cwins.bg/	Търговски регистър и регистър на ЮЛНЦ NRA
Bulgaria	Blockchain-BG	Blockchain-BG OOD	seat and management address: Sofia city, 47a Cherni Vrah Blvd.	www.blockchain.bg	Търговски регистър и регистър на ЮЛНЦ NRA



Recommended documents



- Mapping of SPs and info they can provide
- Requests forms : emergency disclosure requests, preservation of e-data requests, voluntary disclosure request
- Development of “Requesting information from foreign VASPs” Section
- MLA Writer Tool

UNODC trainings on VAs investigations

- Overview of technology-enabled financial crime and associated ML schemes and mechanisms.
- **Collection of financial and digital evidence required for investigations into technology-enabled financial crime.**
- **Dark Web overview: extraction of financial information/scraping, mixers and other obfuscation tools, sale of money mules' cards.**
- Cryptographic essentials: understanding blockchain.
- Encrypted communications, **extraction of financial information from messengers.**
- **Undercover operations into cyber-enabled financial crime.** Possible decryption options.
- Virtual assets basics: virtual assets identifiers as digital evidence.
- Types of cryptocurrency wallets.
- **Blockchain tracing and obtaining information from VASPs.**
- Specifics of banking statement analysis for technology-enabled financial crime.
- **Requesting financial and digital evidence from abroad. Practical scenario on requesting digital and financial evidence (in-country/across borders).**

UNODC trainings on VAs investigations

- Obtaining information from foreign regulated VASPs.
- **Analytical approaches to detection of unregistered Virtual Assets Service Providers (VASPs).**
- Detection of financial activity related to technology-enabled crime and associated money laundering. Required information sources. Use of technical data in financial investigations.
- Money mules syndicates and professional money laundering networks.
- **Using Machine Learning and Artificial Intelligence for detection of financial crime – money mules and BEC accounts example – train model**
- Specifics of freezing, seizure and confiscation of virtual assets – practical tips – seizure from **unhosted wallet**



Work on progressive scenario

- Access illegal marketplace on the Darkweb and get information on BTC addresses used to pay for illicit goods – **simulate “controlled purchase”**
- Use blockchain analysis software to trace transactions and identify the VASP
- Analyse transactions ledgers seized from an underground VASP.
- Combine financial intelligence and technical data
- Draft requests for additional information to foreign service providers (Internet service provider, Airbnb), foreign FIUs and LEAs.
- House search simulation and formulating questions to the digital forensics laboratory.
- Seizure of virtual assets from unhosted wallet, transferring cryptocurrency from the criminal’s address to law enforcement-controlled address.
- Drafting court order for seizure of cryptocurrency from wallet hosted by the VASP.
- Prepare MLA requests with use of UNODC MLA Writer Tool.

UNODC Multilateral EWGs: Virtual Assets

Last EGM: December 2022

In coordination with IEWG VA&TF Project co-lead

Conclusions:

- Terrorist Organizations concerned: Al-Qaeda, ISIL, Hamas Al-Qassam brigades, Hay'at Tahrir al-Sham
- Privacy coins
- Use of obfuscation techniques
- Lack of or inaccurate attribution data - tracing tools' results must be verified
- OSINT skills are important, merging financial intelligence with digital data

UNODC Multilateral EWGs: Professional ML networks

Last EGM: December 2022

Participants: 20 countries, Interpol and Europol

Main trends:

- Use of gold for account settlement by cash controller networks
- Virtual assets + money mules accounts / Hydra Market
- Complex layering schemes (3PML, VAT fraud, grey import)
- TBML and Service-based ML
- Criminal Daigou
- Secured communication platforms, advertisement of services via Darkweb
- Disruption tools (alternative criminal offences, tax measures, undercover ML operations)

Next dates: 18-21 July 2023, focus on PMLs supporting cyber-enabled financial crime, and use of gold by PMLs



Questions for discussion

- Risks and trends you see in current investigations
- Effective detection and financial disruption techniques
- Challenges and ways to raise effectiveness



UNODC

United Nations Office on Drugs and Crime

Thank you!

Aleksandra Bobylkova (Mrs.)

AML/CFT Advisor

Global Programme against Money Laundering,
Proceeds of Crime and the Financing of Terrorism (GPML),

T: +4369914594549 | E: aleksandra.bobylkova@un.org