CyberEast
Action on Cybercrime for Cyber Resilience
in the Eastern Partnership region

Արևելյան Գործընկերություն
Східне партнерство
Eastern Partnership

12 August 2022

Guidelines on the prevention and control of online fraud and criminal money flows

Eastern Partnership

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contents

1 Introduction 4
2 Overview of online fraud and criminal money flow in the region 7
2.1 General Criminal Landscape 7
3 Regional response to online fraud 15
3.1 General comments 15
3.2 Armenia 15
3.3 Azerbaijan 20
3.4 Georgia 24
3.5 Republic of Moldova (Moldova) 30
3.6 Ukraine 34
4 Standard mechanisms for preventing and combatting online fraud and criminal money flows with emphasis of some practices in the region. 40
4.1 Mechanism for reporting on online fraud and criminal money flow 40
4.2 Prevention and public awareness 43
4.3 Risk management measures for prevention and control of online fraud and criminal money flow 43
4.4 Harmonised legal framework based on international standards 46
4.5 Develop adequate skills, resources, and interagency co-operation 47
4.6 Public-private co-operation and information exchange 49
5 Conclusions 54
5.1 FATF Recommendations 54
5.2 Regional Recommendations and Comments 54
5.3 Country Recommendations and Comments 57

In case of need for additional information please contact:

Alexander SEGER
Head of the Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

Abbreviations

AML	Anti-Money Laundering
BEC	Business Email Compromise
CC	Criminal Code
CERT/CIRT	Computer Emergency (Incident) Response Team
CIA	Confidentiality, Integrity, and Availability of ICT systems.
CFT	Countering the Financing of Terrorism
CPC	Criminal Procedure Code
C-PROC	Cybercrime Programme Office of the Council of Europe
CNI	Critical National Infrastructure
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IP	Internet Protocol
IPA	Instrument for Pre-Accession Assistance
ICT	Information Communication Technology
IoT	Internet of Things
ISP	Internet Service Provider
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
MLA	Mutual Legal Assistance
MOF	Ministry of Finance
MOI	Ministry of Interior
MOU	Memorandum of Understanding
MSP	Multi-National Service Provider
OSINT	Open-Source Intelligence
JIT	Joint Investigation Team
SAR	Suspicious Activity Report
NRA	National Risk Assessment on ML/FT
STR	Suspicious Transactions Report
TOR	The Onion Router
URL	Uniform Resource Locator
VPN	Virtual Private Network

1 Introduction

The aim of this guideline is to provide an overview on current standards related to the prevention and control of online fraud and criminal money flows, and provide some future guidelines and recommendations for the priority project countries to consider for the joint CyberEast project of the European Union and Council of Europe.

The report covers the project priority countries of Armenia, Azerbaijan, Georgia, Moldova, and Ukraine. It has been undertaken through desk-based research and subsequent information sharing with the respective countries to add value and clarification.

These guidelines have been prepared in support of the CyberEast Project Result 3 and Output 3.4 respectfully;

- To increase efficient international cooperation and trust on criminal justice, cybercrime, and electronic evidence, including between service providers and law enforcement;
- Implementation of existing agreements on public/private cooperation and conclusion of such agreements in remaining countries.

All the countries listed are parties to the Council of Europe Budapest Convention on Cybercrime (ETS No. 185)[1] and to the Council of Europe Warsaw Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financing of Terrorism (CETS 198)[2]

For the purpose of this report, the definition of online fraud is interpreted as, *a crime in which the perpetrator develops a scheme using one or more elements of the Internet to deprive a person of property or an interest, estate or right by false representation of a matter of fact, whether by providing misleading information or by concealment of information*.[3] To add further context to the standards and guideline in this report, *fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person*.[4]

The main category of proceeds-generating crime on the Internet – as in the real world – is fraud, that is, the intentional deception causing loss of property to another person for economic gain or loss. To ensure that not only traditional fraud committed in the ICT and online environment is criminalised, but also fraud involving interference with computer data and systems, a specific provision on "computer-related fraud" was included in the Budapest Convention on Cybercrime.

In recent years, the project priority countries have sought to build capacity and raise awareness in order the confiscate proceeds from online crime, using bodies such as the FIU, asset recovery units and financial investigation bodies as well as improving interagency and public-private-cooperation.[5]

It should also be noted that the Council of Europe (Moneyval and Global Project on Cybercrime) elaborated a typology study on Criminal money flows on the Internet: Methods, trends, and multi-

[1] https://www.coe.int/en/web/cybercrime/parties-observers

[2] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=198

[3] https://legal-dictionary.thefreedictionary.com/Online+Fraud

[4] https://www.actionfraud.police.uk/what-is-fraud

[5] https://rm.coe.int/1680300aaa

stakeholder counteraction[6]. This study is contributing to raising awareness on current initiatives aimed at preventing and combating cybercrime and money laundering, as well as on proceeds generating offences on the Internet, the report considers the cyber-laundering risks and vulnerabilities and illustrates identified money laundering methods, techniques, mechanisms and instruments of criminal proceeds from cybercrime relying on a number of cases and typologies that were identified and specific indicators of potential money laundering activity within this context.

The FATF Standards set out a range of mandatory requirements that countries must impose on their private sector (through national law, regulations, and other measures). These requirements are collectively referred to as 'preventative measures' and they form the basis for other efforts, including by regulators and law enforcement, to detect criminal finance. These requirements include the collection and retention of personal data (e.g., for identity verification purposes). Specifically on information sharing, the FATF Standards currently require information sharing within the private sector in the context of correspondent banking, processing wire transfers, relying on third parties and implementing group-wide AML/CFT programmes. Among the latest FATF report on collaborating in the fight against financial crime is on data protection, technology and private sector information sharing[7] from July 2022. This report aims to help jurisdictions that are considering enhancing information exchange among private sector entities to design and implement these initiatives responsibly, in accordance with data protection and privacy rules, so that the risks associated with increased sharing of personal data are appropriately considered.

At the time of completing this report, the COVID-19 Pandemic has been actively affecting the global travel and movement of citizens for over twenty months. Examples of these impacts include a significant increase in online purchases worldwide. Next to using payment card data for online transactions on specialised platforms, people started using their actual payment cards and increased mobile phone payments using credit card representations on mobile devices such Apple Pay, Samsung Pay, and Google Pay more and more for in-presence transactions to prevent exchanging physical currency.[8] Some frauds sought to use information connected to the COVID-19 Pandemic to make financial gain through the provision of sub-standard physical products (vaccines, personal protection equipment etc.) and other online scams seeking to defraud or deceive the receiver of the message or information (phishing emails) into making online payments to fraudsters.

The growing e-commerce industry, along with this increase in the online and credit card transactions, were exploited by criminals to an increase of both card-not-present and card-present fraud. While some criminals focused on stealing card details through skimming, phishing, deploying of data-stealing malware and data breaches, others offered for sale this information in illegal "shops" on the Darkweb. Currently, a huge number of card data is available for sale with their legal owners sometimes being unaware of their credentials having been breached.

[6] https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a

[7] https://www.fatf-gafi.org/publications/digitaltransformation/partnering-in-the-fight-against-financial-crime.html?hf=10&b=0&s=desc(fatf_releasedate)

[8] https://www.forbes.com/sites/scarlettsieber/2021/08/27/how-the-pandemic-changed-mobile-payments/?sh=419e03f94315

Additionally, the invasion, following the unjustified and unprovoked aggression by the Russian Federation,[9] against Ukraine has led to significant impact upon the authorities in Ukraine. The Ukraine law enforcement agencies and judiciary have been focussed on differing priorities in the face of the war in their country for seven months. Additionally, some criminal groups have sought to exploit these affairs by defrauding persons overseas on the pretext that transmitted online payments were supporting some initiative to alleviate the impact of the conflict upon Ukrainian communities.

As a main output of this guideline, the current regional threats and trends for online fraud and criminal money flows on the Internet are described internationally and nationally. These threats and trends receive a series of considerations, recommendations and conclusions that could be adopted regionally and, on a country-by-country basis, to continue to build capability in respect of the following;

- To strengthen capability in the reporting, investigation, and prosecution of online fraud;
- To strengthen interagency and public-private cooperation against online criminal money flows on the Internet;
- To increase awareness of the need to confiscate proceeds from crime on the Internet;
- To identify good practices and guidance that could be implemented in project priority countries and areas.

[9] https://www.coe.int/en/web/portal/war-in-ukraine

2 Overview of online fraud and criminal money flow in the region

2.1 General Criminal Landscape

The worldwide growth of, and value of losses attributable to, online fraud has grown exponentially in the last ten years. There are some factors that support these huge increases. The global Internet penetration has increased significantly from 2.3 billion to 5.3 billion of the world's population in ten years to March 2022 with 67.8% of the world now having access to the Internet.[10] Alongside this, technology has developed, and our global business systems have grown alongside these advances, so that humankind now relies significantly upon the Internet and the interconnections it brings.

Connecting ourselves to one another more also means people and businesses are more reachable to online fraudsters operating from different countries across the world than ever before. A situation that will continue to grow for years to come.

One should not just consider the connectivity afforded by computers and servers, but also consider the huge impact made in the development of mobile telephones with Internet connectivity. This has enabled the wide and global usage of online applications and social media, which are often linked to online fraud. There are 5.29 billion unique mobile phone users and 4.55 billion active social media users.[11]

Emerging threats include the wider use of the Internet of Things (IoT), utilising low-cost computing, the cloud, big data, mobile technologies, and physical devices can collect and share data with minimal human intervention. The connected devices include everyday objects such as cars, kitchen appliances, thermostats, monitors, security devices and much more. [12] The risk of cyber-security upon these devices is a significant issue and likely criminal growth area.[13]

Online fraudsters have relied upon the development of their own tools, infrastructure, threats, and trends which, continue to support the growth of online fraud despite heightened cyber-security measures.

2.1.1 Online Fraud Tools

2.1.1.1 Malware

Malware is a generic term that encapsulates all threats (viruses, worms, trojans, ransomware, botnets, etc.), anything malicious that is software related.[14] It is software that is designed to infiltrate or damage a computer system without the owner's informed consent. As computer

[10] https://www.internetworldstats.com/emarketing.htm

[11] https://datareportal.com/reports/a-decade-in-digital

[12] https://www.oracle.com/uk/internet-of-things/what-is-iot/

[13] https://lens.monash.edu/@politics-society/2021/12/01/1384092/criminal-intent-how-the-internet-of-things-can-also-be-a-threat

[14] https://www.fortinet.com/blog/threat-research/evolution-of-malware

systems and applications have changed, so has the growth and development of malware. Currently 560,000 instances of new malware are detected globally each day and aim to infect differing devices, operating systems, or programs.[15]

The development of nation-state malware has now leaked into the criminal infrastructure and are now used to attack technical infrastructure to infiltrate or damage computer systems. In the last ten years, one of the main growth areas of malware has been in the use of ransomware. Aside from ransomware, the evolution from early malware towards the current all-encompassing malware demonstrates the increase in threats; we now see the development and changes of malware attacks have coincided with the development of the hyper-connected world in which we live.[16]

Other developments in malware include the way that it is spread. Traditionally malware is embedded in a file and distributed to a recipient but is reliant upon human interaction to activate the payload and enable the malware to infect the computer or device. Emerging threats include newer methods of spreading malware are seeking to rely less on files or containers to distribute the payload ('fileless malware') and seek to 'piggyback' the code on legitimate scripts. This also makes it harder for users and anti-virus solutions to detect the malware.[17]

The huge growth in malware for mobile devices should be considered as a significant and growing threat vector.

2.1.1.2 **Encryption**

Encryption is the process of encoding data by inputting it with another parameter (key) into an encryption algorithm (cipher). Using either symmetric encryption (single key) or asymmetric encryption (public-private keys), these cyphers are used to protect data at rest, in transit and in use from attackers and/or persons who do not know the keys.[18]

The development and employment of encryption has been used extensively in cyber-security to protect data from attacks and is likely to remain a large growth area in the foreseeable future.

Encryption is also being used extensively by online fraudsters in their communications between one another, whether it is created as a dedicated platform such as EncroChat or common social media platforms such as WhatsApp, Skype, Telegram, and Viber. These types of social media applications have end-to-end encryption and the lawful interception of communications by LEA is seriously impaired because of criminals using these tools and applications. The threat posed by encryption to law enforcement, public safety and national security is raised in several ways, such as failure to obtain evidence needed for investigations, failure to obtain intelligence to avert

[15] https://dataprot.net/statistics/malware-statistics/

[16] https://www.fortinet.com/blog/threat-research/evolution-of-malware

[17] https://us.norton.com/internetsecurity-malware-what-is-fileless-malware..html#

[18] https://id4d.worldbank.org/guide/encryption

harmful attacks and an increase in costs in investigative methods. Key areas include terrorism, online fraud, and child pornography cases.[19]

Other examples of the use of encryption include the use of The Onion Router (TOR) and dark net sites.

2.1.1.3 **Cryptocurrencies**

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit and/or double spend. Many cryptocurrencies are decentralised networks, which use blockchain technology to record transactions on a network of computers owned by users of the system. Cryptocurrencies are outside the control of governments and central authorities and have many legitimate uses. But they are abused for nefarious purposes and examples of cryptocurrencies used by criminals include Bitcoin, Ethereum, Monero. They are used to receive ransomware payments, make purchases on dark web sites and to support the money flow of online fraudsters.[20]

In 2021, cryptocurrencies were sent to illicit addresses to a value US$14 billion, which increased significantly over the course of the year, up from US$7.8 billion in 2020.[21]

It should also be noted that blockchain technology is an emerging subject, where understanding will be needed by LEA and the judiciary outside of the current scope of financial investigations and money laundering. Visions for the future use of the World Wide Web, include Web 3.0, which will be based upon blockchain technology, utilising it for integrity and security purposes.[22]

2.1.1.4 **Botnets**

A botnet is a collection of compromised computers, that have been infected by malware. This enables criminals to access and remotely control the computers utilising a command-and-control structure. A growing area of infected computers and devices includes the IoT.

Botnets have historically been used to send spam emails, click fraud campaigns and to undertake distributed denial of service (DDoS) attacks.[23] It is noted that the number of DDoS attacks are decreasing, but those that are being conducted have grown in scale and complexity.[24]

Another significant and growing criminal area of the criminal use of botnets is crypto jacking. This is the unauthorised use of a computer or computers to mine cryptocurrency. It is likely that the

[19] https://www.ojp.gov/ncjrs/virtual-library/abstracts/encryption-and-evolving-technologies-tools-organized-crime-and

[20] https://www.investopedia.com/terms/c/cryptocurrency.asp

[21] https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

[22] https://www.forbes.com/sites/forbestechcouncil/2022/05/12/a-vision-for-the-next-generation-of-the-world-wide-web/?sh=6d89407e2799

[23] https://www.techtarget.com/searchsecurity/definition/botnet

[24] https://securitybrief.com.au/story/ddos-attacks-are-becoming-increasingly-large-and-complex

user will not notice any impact upon the services provided by their device, beyond a potential slowdown as the unauthorised attacker employs resources such as the processor and RAM to solve the calculations involved in mining crypto currencies.[25]

2.1.2 Cybercrime infrastructure

2.1.2.1 Proxies and Virtual Private Networks (VPN)

Proxy servers provide many legitimate uses for network and computer security and efficiency, which in turn reduces costs. They can be used to improve security through the provision of web filters or firewalls or limiting employees' Internet activity, preventing snooping by adversaries. Other uses include balancing Internet traffic to prevent system failure, caching files or compressing traffic to reduce bandwidth overheads.[26]

Illegal uses of proxies include persons hiding their locations by routing traffic through a proxy server to conceal IP addresses, thus reducing the risk of identification and attribution.

A VPN is a provided service that establishes a secure and encrypted connection between the user's device and the Internet (often referred to as tunnelling). A VPN will route traffic through other services so that the user's IP address is hidden from the website or service to which they connect. The added benefit of encryption means that not only the IP address remains concealed, but the content is also protected.[27]

There is now widespread usage of VPNs, and this includes the criminal use. Many criminals use VPN as an additional measure of protection even when connecting to dark web sites on TOR. The choice of VPN IP addresses in many countries around the world, together with concealment of the user IP addresses along with end-to-end encryption makes VPNs an attractive tool for online fraudsters.

Many VPN service suppliers do comply with lawful requests for data communication details, so long as they comply with legal frameworks. But it should be remembered that many users of VPNs are legitimate users seeking to protect their data from snoopers and criminals or are seeking to access services that they can only access in another jurisdiction.[28]

2.1.2.2 Darkweb sites on TOR (Underground Economy)

TOR was a concept designed initially by the US navy and is now managed by a not-for-profit organisation in the USA called The Tor Project, Inc. It allows users to connect to a network of computers identified as nodes by downloading and utilising software onto a local device. The software enables connection to an entry node, which then passes onto a few intermediatory nodes before reaching the exit nodes allowing communication to a resource on the Internet.

[25] https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

[26] https://www.fortinet.com/resources/cyberglossary/proxy-server

[27] https://www.avast.com/c-what-is-a-vpn

[28] https://www.nstec.com/do-criminals-use-vpn/

At each node a layer of encryption is added, meaning several layers of communication are added, before being decrypted at the exit node. The layers are represented as the differencing layers of an onion. Nodes are typically run by volunteers.[29]

Dark web sites use the facility of hidden services on the TOR network to conceal their physical location through the concealment of IP address. For each hidden service, a descriptor is created, and the TOR network allows communication with the user to take place using intermediatory rendezvous points on the TOR circuit. Locating the actual service is not possible using traditional investigative methods.[30]

Dark web sites descriptors (TOR URLs) that are used in cybercrime and online fraud are often identifiable through OSINT on the World Wide Web. Various indices will provide the descriptor, which can be entered into the TOR browser and connection can be made. This is not necessarily the case in terrorism and child abuse sites.

Most dark web sites will require the user to create a profile and transfer some cryptocurrency into their profile account before allowing purchases. The cryptocurrency value is transferred to the administrator's cryptocurrency wallet until a transaction is made and the value is transferred after completion of the sale (commonly referred to as 'escrow') to the vendor.

Certain dark web sites are interested in single subject matters, such as drug sites, terrorism sites and child abuse sites. Online fraud sites are often mixed with a variety of other offerings including firearms, drugs, malware, malware as a service, botnets for hire, and more besides. Typical fraud offerings include online bank login data, credit card data for online purchases, magnetic strip data for the back of physical bank cards, various account usernames and passwords and mules and cash out offerings.

Investigation and prosecution of administrators and vendors on websites is a complex area, often requiring advanced levels in covert operations and OSINT, along with advanced technical capabilities. However, through numerous collaborative investigations some significant successes have seen the arrest and prosecution of many administrators of dark web sites and the closure of the sites themselves.

2.1.2.3 **Bulletproof hosting**

Bulletproof hosting operations are like regular web hosting; however, these hosting companies are a lot more lenient or permissive about what can be hosted on their servers. They utilise somewhat of a "don't ask, don't tell" philosophy.

Bulletproof hosting services are often found in countries with more relaxed laws and enforcement about what type of content is hosted on these servers, therefore making it easier to evade capture. Due to the different laws in different countries, this creates a huge grey area that allow the owners

[29] https://www.torproject.org/about/history/

[30] http://www.cs.sjsu.edu/faculty/pollett/masters/Semesters/Fall13/akash/Tor_HiddenService.pdf

to claim immunity to what their customers host. These hosting operations can be used to host exploit kits, nefarious data storage and dark web sites.[31]

2.1.3 Threats and trends

There are numerous methods to exploit and defraud businesses and individuals. They are reliant upon technology to communicate the deception to the victim and are often underpinned with social engineering skills. Some rely on technical matters such as the building of a criminal infrastructure or use of malware.

There are many differing types of online frauds not described within this report. The threats and trends reported below relate to the most common online frauds impacting upon law enforcement within the region.

2.1.3.1 Business email compromise

BEC is where criminals gain unlawful access to email systems or use social engineering skills to gain information about corporate payment systems and then deceive company employees into transferring money to the criminal's bank account, which they believe to be a genuine account belonging to an associate, supplier, customer, or other similar party.

Methods employed by the criminals to gain access to email systems include spear phishing messages, other targeted social engineering attacks and malware.

When the criminals send the message about transferring the money, it will often be supported with some type of documentary support, such as an invoice or a bill with all the normal company letterheads. The messages are often received near to the close of the working day and reinforced with some type of urgency meaning the payment needs to be made immediately. The criminals often purport to be a person in authority (such as a manager or senior person) and seek confidentiality making it less likely for the recipient to check the validity of the message.[32]

Once the criminals receive the funds, the money is quickly transferred across international bank accounts. This often involves dedicated money launderers and mules.

In the USA, the value of losses over a five-year period to June 2021 for BEC crimes totalled over US$43 billion.[33]

2.1.3.2 Card not present fraud

Card not present frauds occur when a criminal(s) use compromised credit or debit card details to buy something on the Internet, over the phone or through mail order.

[31] https://us.norton.com/internetsecurity-emerging-threats-what-is-bulletproof-hosting.html

[32] https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud

[33] https://www.techrepublic.com/article/fbi-43-billion-losses-are-business-email-compromise-fraud-between-2016-2021/

It is reported that card not present fraud continues to rely upon criminals using credit card details obtained through third-party data breaches and via phishing emails and scam texts. The card details are then sold to other criminals through mediums such as dark web sites on TOR.

Methods of transferring the illegally obtained goods into money, include onward selling of them through social media.

Another method includes the use of social media to advertise discounted items and when a victim orders the goods online and makes the card payment to the fraudster. The fraudster keeps that 'discount payment' and then uses the supplied card details to make an order to the real supplier for the goods to be delivered to the victim.

It is reported that additional compromises and risks have occurred during the COVID-19 pandemic, when more online transactions were made with credit and debit cards globally.[34]

2.1.3.3 **Charity donation fraud**

Fraudsters take advantage of generosity of members of the public through the raising of money for a fake charity or cause. Most of these charity donation frauds rely upon current news stories that are circulating and then seek to exploit that generosity.

Current examples that are available at the time of reporting include warnings of frauds, where victims are being contacted by phone, email, and social media to make charity donations in support of Ukrainian refugees.[35]

2.1.3.4 **Money mules**

Money mules are recruited, sometimes unwittingly, by criminals to receive and transfer illegally obtained money between bank accounts. The mules typically receive the stolen funds into their account and are asked to wire the money to a different account, often one overseas whilst keeping some of the money for themselves.

Money mule networks advertise roles in job adverts, social media posts promising large amounts of money for little work or investment.[36]

Money mule networks are advertised for the use of criminals to support their money flows, often with a cost of 40% of the money that is being received and transferred.

[34] https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

[35] https://www.orilliamatters.com/police-beat/police-warn-of-charity-scam-targeting-donations-to-ukraine-5214455

[36] https://www.actionfraud.police.uk/a-z-of-fraud/money-muling

Money mule adverts often target persons under 35 and persons who have only recently entered the country in which they are resident. Over 90% of money mule transactions are linked to cybercrime and online fraud.[37]

2.1.3.5 **Phishing**

Most cyber-attacks start with phishing emails, enticing someone to click on a malicious link or deceiving them into revealing their credentials for a financial or online service. Businesses report that there has been a continual increase in cyber-security breaches over the last five years, with some quoting a 67% increase. Worryingly, the increase in cyber-attacks shows no sign of slowing down.

Many phishing attacks aim to steal, change, or destroy data. An added consideration is that almost all ransomware attacks commence with a phishing email that someone in the targeted company activates by unwittingly clicking on a malicious link. Statistics released by the USA FBI indicate that more than 156 million phishing emails are sent every day and 16 million get through email filters. Of these around half are opened by recipients.[38]

Whilst most phishing attacks are sent to a very large number of people, only a small percentage will respond. But spear phishing emails are carefully designed to get a single recipient to respond. Criminals will undertake OSINT research using social media and other public information and create an email tailored for that person. Because of the OSINT and the personal details included in the spear phishing email, it is more likely that a person will respond and become a victim of online fraud.

[37] https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

[38] https://www.inky.com/en/blog/what-a-phishing-attack-costs-your-business

3 Regional response to online fraud

3.1 General comments

This section aims to give an overview of the current responses, landscape, legal framework, and public private partnership in relation to online fraud and criminal money flows in the project priority countries. The purpose of providing this information is to support a comparison between what occurs regionally and international best practice to make informed and evidence-based conclusions.

Because of the international connectivity, it is fair to assume that many criminal attacks and trends will be very similar throughout the region. However, there are local criminal issues to consider, and geo-politics also have some impact upon cyber-security and cybercrime. The response often depends upon national priorities, available resources and current capacities in the various entities tasked with prevention, investigation, and prosecution of cybercrime.

3.2 Armenia

3.2.1 **Criminal landscape – national factors**

Armenia has a total population of around 3 million citizens of which over 2 million are Internet users. Internet growth has been increasing by about 5% per year, whilst the use of social media has increased by 20% between 2020 and 2021 to over 1.8 million citizens. The use of credit cards by citizens in the country is low (8%) and conducting online purchases amongst citizens is increasing (15%)[39]

Armenia has no formal cybersecurity or cybercrime strategy in place, but the National Security Service is responsible for cybersecurity and protection of government networks. Armenia has found itself the subject of cyber-attacks against its ICT from foreign states, international terrorist organisations, criminal groups, and individuals.[40]

Whilst Armenia did find itself subject of some cybercrime targeting individuals and business, it was at a comparatively low rate until 2020, with some low-level online fraud operating at a local and national level being conducted through social media and alike. There were other attacks, from international origins, which have been infrequently reported;

- In 2017, banks in Armenia were subject of spear phishing email attacks;[41]
- In 2019, rival criminal gangs in Turkey and Azerbaijan have previously reported hacking into rival websites over disputes between governments of Armenia and Azerbaijan;[42]
- In 2019, the police identified a crime group located in Yerevan operating a technical support scam, where the fraudsters purported to be working for an international company. The criminals contacted unwitting victims in various countries purporting to support their

[39] https://datareportal.com/reports/digital-2021-armenia

[40] https://www.dcaf.ch/sites/default/files/publications/documents/ArmeniaCybersecurityGovernanceAssessment.pdf

[41] https://securityaffairs.co/wordpress/65061/cyber-crime/silence-group-bank-attacks.html

[42] https://www.hackread.com/cyberwar-turkish-vs-armenian-hackers/

devices, making demands for their services, and stealing personal data of USA and Canadian citizens. The group, made up of Indian and Armenian nationals were arrested and prosecuted by authorities;[43]

- In 2020 the rate of cyber-attacks including state sponsored attacks began to increase (even before the war with Azerbaijan).[44]

Currently cybercrime reporting in Armenia remains quite low, when compared to other countries in the region.

3.2.2 Legal Framework

3.2.2.1 Cybercrime and online fraud

Whilst there is currently no dedicated strategy or action plan on cybercrime, there is ongoing work to develop a comprehensive cyber-security strategy for Armenia. The Digitalisation Strategy of Armenia was adopted in 2021 and includes measures regarding cyber-security, legal framework, and data protection.[45]

Armenia has adopted the new Criminal Code of the Republic of Armenia (CC) and the Criminal Procedure Code of the Republic of Armenia (CPC), which came into force on 1st July 2022. The new legislation contains elements of all of the substantive law offences provided by the Budapest Convention on Cybercrime.

The articles in the Chapter 38 (Articles 359 – 365) of the Armenian CC adequately deal with the main cybercrime offences described in the Budapest Convention on Cybercrime. Specifically, Article 364 of the CC covers online fraud, whereby illegally inputting, modifying, deleting or blocking (isolating) computer data for the purpose of causing legal consequences, which led to creating unreliable data shall be punished by a fine for maximum, or public works for a term of eighty to one hundred and fifty hours, or deprivation of the right to hold certain positions or exercise certain activities for a term of two to five years, or restriction of liberty for a term of maximum two years, or short-term imprisonment for a term of maximum two months, or imprisonment for a term of maximum two years.These offences are further supported by Article 257[46], which criminalises fraud by means of a computer and appears to criminalise the illegal appropriation of non-tangible items (such as cryptocurrencies).

[43] https://armenpress.am/eng/news/973297

[44] https://media.am/en/critique/2022/06/01/33065/

[45]https://www.coe.int/en/web/octopus/-/armenia?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_HWAFAbhgD3hQ&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

[46] Article 257 of the CC criminalizes theft committed by means of computer, i.e. the illegal taking of someone's property, which has been committed by entering, altering, destructing, blocking (isolating) computer data without provided by law, or contract or other legitimate ground, or by influencing the operation of the computer, computer system or computer network in any other way shall be punished by a fine in the amount of ten-fold to thirty-fold, or public works for a term of one hundred to two hundred hours, or restriction of liberty for a term of maximum two years, or short-term imprisonment for a term of maximum two months, or imprisonment for a term of maximum three years.

3.2.2.2 **Money Laundering.**

Articles 295 – 296 describe the offences related to money laundering offences and forfeiture. Article 121 deals with confiscation and describes criminal property as follows.

> *property, income or other types benefits are any material goods, movable or immovable objects of civil law, including financial (monetary) means, payment instruments, securities and property rights, documents or other means verifying the property rights, the interest received out of the property or interests accrued on it, the dividends or other income, as well as related rights and patent rights.*

Paragraph 10 of Article 121 of the CC defines goods, income and other types of benefits as any kind of material goods, movable or immovable objects of civil law, including financial (monetary) means, payment instruments, securities and property rights, documents or other means verifying property rights, the interest received out of the property or interests accrued on it, dividends or other income, as well as related rights and patent rights.

Thus, the definition of goods under the criminal legislation is broad enough to cover virtual currencies. The definition of assets stipulated under Article 3 of the Civil Forfeiture Law includes direct reference to cryptocurrencies.

3.2.3 **Criminal justice response**

The High-Tech Crime Department of the National Police is a centralised unit dedicated to handling cybercrimes across Armenia. This unit receives the initial report and undertakes first steps before disseminating the matter of official investigation to the Investigation Committee.

The Investigation Committee is an independent body, which carries out 96% of the criminal cases in Armenia. In 2019 a Department of Investigation of Cybercrime and High Technology Crime was founded to respond to the increasing rates of reported cybercrime cases. The unit, which is within the auspices of the General Department of Investigation of Important cases, deals with almost all of the cybercrime cases within Armenia. As well as its investigative capabilities, the department also contains a dedicated Digital Forensic Laboratory, which leads in examination, analysis and reporting about all computer systems that are subject of investigation in the Investigative Committee.

Armenia has a dedicated administrative financial intelligence unit called the Financial Monitoring Center, within the structure of the Central Bank of Armenia.

The Government Computer Emergency Response Center (cert.gov.am) collects and analyses the data regarding cyber incidents in regards to state entities. The Government CERT shares information and provides guidance regarding ongoing and current threats to state entities. It supports the information sharing processes with further measures to prevent cyber incidents. Where cyber incidents are reported to the Government CERT, the response team actively cooperates with the entities and law enforcement authorities as necessary.

There is no information to identify whether the entities involved in cybercrime, online fraud, online financial investigations, and electronic evidence have adopted a meaningful training strategy. These entities include law enforcement agencies, prosecutors, and judges.

However, over 70 investigators within the Investigative Committee has received training in relation to online financial investigations, electronic evidence handling and dedicated case studies where learning about technology is provided.

3.2.4 **Public private cooperation.**

Strategic cooperation and coordination of national AML/CFT policies is conducted through the Standing Committee on Combating Money Laundering, Terrorism Financing and Proliferation Financing, established by the Decision of the Prime Minister of the Republic of Armenia.

At the operational level, the Financial Monitoring Centre (FMC) is actively cooperating with LEAs in the context of information exchange, implementation of preventive measures and detection of potential online frauds and criminal money flow or potential ML/FT cases. The FMC notifies LEAs, when based on the analysis of a report filed by a reporting entity or of other information in the manner established by AML/CFT law, it arrives at a conclusion on the presence of reasonable suspicions of money laundering or terrorism financing, or such reasonable suspicions on a predicate offence that could result in money laundering.

The number of requests from LEA to FMC has seen a slight increase to 2021.[47] When handling requests from LEA, the FMC makes necessary requests not only to the financial institutions in Armenia but also to foreign FIUs.

The cooperation of the FMC with the private sector (obliged entities) is undertaken through meetings so that they are actively participating in developing regulation and guidelines to mitigate a higher risk of ML/FT. In recent period, the FMC has issued instructions on taking preventive measures against fraudulent schemes and persons possibly involved in them.

The FMC has regularly provided feedback to the commercial bank on the analysis carried out and measures taken based on STR received by the banks. The FMC provides guidance and training to the private sector and other authorities on a regular basis. In the last Moneyval evaluation report it was noted that Chamber of Advocates expressed a need for further training in AML/CFT, which indicates that co-operation can be strengthen further. Since the last MONEYVAL evaluation, numerous trainings with various domestic partners, including Chamber of Advocates have been conducted. The FMC frequently update its website with useful information on an amended list, which includes updated typologies and guidance for the obliged entities.

The Central bank has a “warning” section to notify the public on some identified activity in the financial system. There is a special website (www.abcfinance.am) created by Central Bank of the

[47] The number of requests made by law enforcement authorities to the FMC has somewhat increased in comparison to the previous year, reaching 575 in 2020 and around 630 in 2021.

Republic of Armenia as a financial education online platform. It presents useful information, videos, and graphics which raises public awareness about differing online frauds and Ponzi schemes.

On 23 November 2015 the Investigative Committee signed a MOU[48] with ArmenTel, K-Telecom, UCom, and Orange Armenia with the intention to streamline processes. In this framework, the parties agreed to communicate on a standardised manner (including cover letters, electronic signatures) and to cooperate to remove blockages and solving other issues as quickly as possible to expedite procedures. Practically, the MOU achieves a same day request-answer working model. The cooperation on data aims to remove any friction in obtaining evidence under legal processes. It does not seek facilitating the exchange of facts outside of the legal process.

Academic institutions and experts play an active role in education on cybercrime, and they support the work of the LEA on an occasional basis.

[48] The main intentions of the Memorandum are to take effective joint measures in the direction of operative transmission of court decisions and transcripts, and to develop the cooperation on introduction of technical capabilities.

3.3 Azerbaijan

3.3.1 Criminal landscape – national factors

Azerbaijan has a total population of around 10 million citizens of which over 8.26 million are Internet users (81%). Internet growth has been increasing by about 2.5% per year, whilst the use of social media has increased by 16% between 2020 and 2021 to over 4.3 million citizens. The use of credit cards by citizens in the country is very low (5%) and conducting online purchases amongst citizens is also low (9%).[49]

Azerbaijan has implemented a cyber-security strategy for 2019-2022 and plans to adopt a new strategy from 2022 to 2027. A presidential decree was issued in 2021 giving the outline requirements for the new cyber-security strategy, which included increasing the capacity of the State Security Service to enable it to undertake additional functions to deal with cybercrime. Other indications are that increase security standards are going to be legislated and implemented in the protection of computer networks in the public and private sectors, continuing with improving standards outlined in earlier strategies.

In April 2022 a new public association was created to unite companies, organisations and specialists operating in the country in the field of ICT. The Association of Cyber-security Organisations of Azerbaijan (AKTA) aims to support the application of scientific and technical achievements in cyber-security, awareness and protect national interests from propaganda and disinformation.[50]

Azerbaijan has a relatively low rate of reporting of cybercrime, but this does not mean that significant investigations do not take place. Furthermore, the COVID-19 pandemic required more people to work from home and consequently reported cybercrime increased notably. The offences linked to the time people were working from home included social engineering attacks to support online fraud and the deployment of ransomware.[51]

Notable investigations include the following;

- In November 2019, 44,000 IP addresses belonging to Azerbaijani nationals were illegally used to mine Monero cryptocurrency. It was identified that 3,500 differing devices were infected with malware. The mined cryptocurrency was sent to IP addresses in Canada and the UK;
- In March 2022 online fraudsters were distributing fake iOS applications for Apple devices to spread malware and bypass security on the device allowing them to make unauthorised payments from online banking accounts. The suspects were identified as an Azerbaijani criminal group using the name Cryptorom.[52]

[49] https://datareportal.com/reports/digital-2021-azerbaijan

[50] https://www.azernews.az/business/195577.html

[51] https://www.coe.int/en/web/cybercrime/-/cybereast-interview-on-the-work-of-a-cybercrime-investigator-with-the-state-security-service-of-the-republic-of-azerbaijan

[52] https://eng.az24saat.org/2022/03/20/fraudsters-used-this-method-to-steal-money-from-the-account/

3.3.2 Legal Framework

3.3.2.1 Cybercrime and online fraud

The Criminal Code of Azerbaijan contains elements of all substantive law offences provided by the Budapest Convention on Cybercrime.

The Code of Criminal Procedure does not implement any procedural powers in compliance with the Budapest Convention on Cybercrime except for production orders (Article 18). There are several previously reported gaps in the legal framework in relation to;

- Article 16 - Expedited preservation of stored computer data;
- Article 17 - Expedited preservation and partial disclosure of traffic data;
- Article 19 – Search and seizure of stored computer data;
- Article 20– Real time collection of traffic data;
- Article 21 – Interception of data.

3.3.2.2 Money Laundering.

The Criminal Code provides limited legal framework regarding money laundering in relation to online fraud and other criminal offences. There appears to be strong legislation to deal with terrorist financing and financial gains made through drug trafficking. Article 51 of the Criminal Code deals with the confiscation of property, where it is gained during the commitment of a crime but does not tend to deal with matters where it is concealed, transferred, or exchanged into another representation. Article 194 of the Criminal Code deals with the purchase or selling of the property extracted obviously in the criminal way.

The Criminal Code does not appear to reference to non-tangible items such as cryptocurrencies, digital currencies, and virtual currencies. There are no definitions to indicate whether they are included in description of "property."

The Code of Criminal Procedure has limited scope to deal with money laundering investigations. Chapter XXXII contains Articles 248-254, which relate to the Attachment of Property. This gives powers to confiscate property according to provisions of the criminal law, but there appears to be minimal legal framework to support financial investigations. Matters such as search, seizure, and production orders in relation to financial institutions do not appear in the criminal code and it is unclear how investigators obtain evidence relating to concealment, transfer and possession of assets obtained by criminal ventures such as online fraud.

There are no meaningful description of funds or other assets to identify that cryptocurrencies, digital currencies, and virtual currencies in the Code of Criminal Procedure. If these are not included in any definition, the search, seizure, and confiscation of criminal assets, which are represented in digital form, could be undermined.

3.3.3 Criminal justice response

The Department of Combating Crimes in Communications and IT of the Counter-intelligence Provision of the Economy at the State Security Service leads the main response to cybercrime and online fraud.

The Cyber Security Service (CERT-AZ) performs the role of the national CERT. It engages in coordinating action and responses to attacks on infrastructure, reporting risks and vulnerabilities, and aiding public and private sectors in areas of cyber-security.

The Computer Emergency Response Center (CERT.GOV.AZ) is responsible for cyber-security for state and government computer networks.

There is no information to identify whether the entities involved in cybercrime, online fraud, online financial investigations, and electronic evidence have adopted a meaningful training strategy. These entities include law enforcement agencies, prosecutors, and judges.

3.3.4 **Public private cooperation**

The Coordination Council is chaired by the Deputy Prime Minister of the Republic of Azerbaijan and contains representatives of other relevant bodies. Its main purpose is understanding AML /CFT risks at the national level, setting strategic targets for risk mitigation, and taking steps to reduce the risks identified in NRA.

The Financial Monitoring Service (FMS) is Azerbaijan's financial intelligence unit and was established as a public legal entity to strengthen the capacity of government agencies and create an effective coordination mechanism of activities in this area. Other objectives include increasing the efficiency of cooperation and information exchange between FMS and government agencies, and to expand international cooperation in measures taken in the field of AML and CFT.

In its annual reports, the FMS identified it received significant and tangible information from reporting entities and intelligence, which were analysed and then submitted to the Prosecutor General's Office and State Security Service for investigation. LEA also submit inquiries to the FMS, which require investigation before relevant details are submitted to the relevant agency.

The FMS has received several requests from private sector, mainly from reporting entities related to the interpretation of the AML legislation. The FMS has held several meetings with the representatives of the monitoring entities during which various topics of the AML/CFT sphere were discussed and where necessary action or improvements made. FMS posts draft legislation on its official website for comments from the private sector.

FMS have introduced a modern e-learning platform for teaching-learning process, which include new innovative approach concerning AML/CFT. Trainings sessions organised by the FMS have been used for discussions on preparation of new AML/CFT laws, regulations, guidelines, etc.

In the Banking Association there is an expert group assigned to work on compliance. The expert group is involved in discussing the compliance alongside the requirements of AML and compliance legislation of Azerbaijan Republic, the demands of the international conventions that are acceded by the country, recommendations of Financial Action Task Force (FATF), Basel Committee principles on Banking Supervision and requirements of Financial Monitoring Service under the Central Bank of the Republic of Azerbaijan. The group aim is to agree on methods to improve and unify standards of internal control system of banks, review the opportunities to form a regime that prevents the possibilities of financing the terrorism and legalization of criminally gained money and other properties.

The FMS publishes information on its official website that includes:

- Events in which it has participated;
- Guidelines, typologies, and indicators relevant to AML and CFT;
- Current or recent crimes affecting citizens relating to online fraud and cyber interference.[53]

There is lack of systematic efforts to raise the financial literacy and consumer protection, which could focus on public awareness for the online fraud, cybersecurity, such as a series of simple educational videos, or multimedia intended raising for the raising of the public awareness. Usage of social media platforms could be used to reach younger population to avoid identified risks that they may be recruited as money mules.

There is currently no agreement between Government of the Republic of Azerbaijan and ISPs within Azerbaijan. There is a general legal obligation upon ISP's to cooperate under Article 39 of Law of the Republic of Azerbaijan on Telecommunications, which tasks all communication providers to set up suitable conditions for carrying out operative-search activities by authorized state agencies, in particular, to "promote in proper legal manner implementation of search actions, supply telecommunication networks with extra technical devices according to terms set by corresponding executive power body for this goal, solve organizational issues and keep methods used in implementation of these actions as secret."

[53] http://fiu.az/typologies

3.4 Georgia

3.4.1 Criminal landscape – national factors

Georgia has a total population of around 4 million citizens of which over 2.74 million are Internet users (77.8%). Internet growth has been increasing by about 9.5% per year, whilst the use of social media has increased by 14.8%% between 2020 and 2021 to over 3.1 million citizens. The financial inclusion of the country is 61%, which suggest that ownership of payment cards is at least at that level, but ownership of payment credit cards by citizens in the country is low (around 14.6%) and conducting online purchases amongst citizens is also low (in volume this type of transaction represent around 13.5% of total volume of all card transactions).[54]

Georgia had implemented two previous national cyber-security strategies covering the period of 2012-2018, but the country continued without implementing a successive plan until 2021. Georgia is implementing its third national cyber-security strategy for 2021-2024, which establishes four priorities;

- Developing an information society;
- Resilient cyber security governance system and strengthening public-private partnership;
- Enhancing cyber capabilities;
- Strengthening Georgia's position, as a net contributor to cyber-security.

The strategy, which was approved by the Georgian Government in September 2021 identified two main threats facing the country;

1. Cyberwar and other attacks run by state actors;
2. Cybercrime, including attacks on CNI.[55]

The National Cyber-Security Strategy reported that the key threats of cybercrime originate from phishing, ransomware, defacement of websites, DDoS, and mail spoofing (business email compromise).

According to the Georgian national strategy, the state actors causing the biggest threat to Georgia originate from the Russian Federation. By example in 2019, the government of Georgia, alongside international partners, identified and dealt with a large-scale, disruptive cyber-attack carried out by the Russian Federation Main Intelligence Directorate (GRU) against Georgian infrastructure, including the court system, non-government organisations, media, and other private businesses.[56]

Reports have identified that cybercrime is an emerging phenomenon in Georgia and the threat is not properly perceived either by government or the society. It is also recognised that cybercrime is underreported (like other countries in the region) and from the perspective of criminal justice, policies relating to cybercrime do not attract sufficient investment due to the low significance in national criminal statistics. It is estimated that cybercrime in Georgia is increasing by 25% year-on-year.[57][58]

Notable investigations include the following;

[54] https://datareportal.com/reports/digital-2021-georgia

[55] https://civil.ge/archives/446772

[56] https://www.gov.uk/government/news/new-uk-support-to-protect-georgia-against-russian-cyber-attacks

[57] https://www.pmcresearch.org/policypapers_file/f599606315041911a.pdf

[58] https://pmcg-i.com/publications_show/324/Cybercrime-in-Georgia:--Current-Challenges-and--Possible-Developments

- In May 2019 an unprecedented, international law enforcement operation involving USA, Bulgaria, Georgia, Moldova and Ukraine, which dismantled an organised crime group involving bullet proof hosting and the spread of the GozNym malware to over 41,000 computers targeting online banking login credentials. The collaborative organisation was able to target Russian speaking criminal forums, who were also using other services such as money mules, spammers, crypters and organisers. The prosecution and conviction of the main two offenders occurred in Georgia and others were successfully prosecuted in the USA.[59]
- In June 2020 police detained a man who had illegally accessed 25 separate social media accounts and then wrote to contacts and friends of the account holders, deceiving the contacts into making payments and providing financial data such as bank account information;[60]
- In January 2021 police detained an Indian national in Tbilisi for illegally accessing computer systems and misuse of data. He conducted several small frauds which resulted in financial gains of €2,300 Euros, which he withdrew from an ATM machine in cash;[61]
- In October 2021 a collaborative international investigation in partnership with Israel, Germany and Eurojust saw the arrest of several suspects in Georgia undertaking a complex online investment fraud. Victims lost all their investments to the criminal gang and the police recovered real estate, cars, and cash during the arrests.[62]

3.4.2 Legal Framework

3.4.2.1 Cybercrime and online fraud

The Criminal Code of Georgia contains elements of all substantive law offences provided by the Budapest Convention on Cybercrime.

The Criminal Procedure Code generally implements procedural powers in compliance with the Budapest Convention on Cybercrime and is one of the few countries in the region that has complemented its legislation with provisions for international production orders.

3.4.2.2 Money Laundering.

The Criminal Code Article 52(3) Confiscation of property allows the Court to confiscate criminally obtained property (which includes all property and intangible assets as well as title deeds for property) at the time of sentencing if the asset can be linked to crime.

The Criminal Code Article 194 deals with legalisation of illegal income (money laundering) and deals with all the main offences related to individuals undertaking money laundering activities. [63]

Whilst there is no reference to intangible property in this article, clarity on the matter is provided through Article 147 of the Civil Code of Georgia, in which the concept of property is described for all legal proceedings to include all things, tangible and intangible. Based on this definition, assets that exist in electronic forms are included in crimes stipulated in Article 194.

The Criminal Procedure Code provides scope to deal with money laundering investigations. Articles 151-158 give powers to confiscate property according to provisions of the criminal law.

[59] https://www.eurojust.europa.eu/news/goznym-malware-cybercriminal-network-dismantled-international-operation

[60] https://agenda.ge/en/news/2020/1779

[61] https://agenda.ge/en/news/2021/187

[62] https://www.eurojust.europa.eu/news/support-arrest-online-scammers-georgia-and-israel

[63] https://matsne.gov.ge/en/document/download/16426/157/en/pdf

The Criminal Code Article 52(3) Confiscation of property allows the Court to confiscate criminally obtained property (which includes all property and intangible assets as well as title deeds for property) at the time of sentencing if the asset can be linked to crime.

The Criminal Procedure Code of Georgia envisages confiscation of property as a measure of coercion during criminal proceedings. The criminal procedural legislation of Georgia does not define the concept of property, however, according to the civil legislation of Georgia, property includes both material and immaterial goods, therefore seizure may be made on the property that exists or is represented in electronic form.

Insofar as non-conviction-based confiscations (NCC) are concerned, these have been in use in Georgia since 2006. It is governed under Chapter XLIV1[64]of the Code of Civil Procedure. NCC is used in respect of most serious select crimes such as drug trafficking, human trafficking, corruption, serious organized crime, etc.,).

NCC can be sought in respect of assets that are undocumented or ill-gained and reasonable link can be established with a specific crime. "Balance of probabilities" is the pertinent standard of proof as opposed to "beyond reasonable doubt" the latter being applicable in criminal trials. Some tens of millions of assets have been recovered through these procedures. Civil litigations unit of the Office of the Prosecutor General is responsible for civil non-conviction-based confiscations.[65]

3.4.3 Justice response

The Cybercrime Division of the Central Criminal Police Department at the Ministry of Internal Affairs lead the main LEA response to cybercrime and online fraud.

The Regional Police Department in Tbilisi established a cybercrime division, which works in a similar way to the unit division in the Central Criminal Police Department. Other regional police departments are improving capacity to handle cybercrime, online fraud, and cyber enabled cases, where electronic evidence is found.

Recently the Office of the Prosecutor General has set up Cybercrime Unit which is responsible for the investigation and prosecution of most serious cybercrimes as well as the recovery of virtual assets.[66]

The Georgian Research and Educational Networking Association (GRENA) undertakes the role of the national CERT (CERT-GE). It provides ICT information, training, and awareness within Georgia. It engages in consultation and responses to attacks on infrastructure, reporting risks and vulnerabilities and aiding public and private sectors in areas of cyber-security.

[64] https://matsne.gov.ge/ka/document/view/29962?publication=149#!

[65] Details provided by Ministry of Justice in Georgia

[66] Provided by Georgian MOJ upon review

According to the Georgian Prosecution Service Strategy 2022-2027, trainings on cybercrime, electronic evidence and recovery of virtual assets are high priority. Under this new strategy and action plan the prosecution service plans to deliver basic cybercrime and electronic evidence training to all prosecutors within the lifetime of the strategy.

At the time of reporting, the Prosecution Service of Georgia employs 475 prosecutors and 120 investigators. Of these, 17 specialised prosecutors and investigators will continue an intensive program involving advanced electronic evidence, darknet investigations, understanding virtual assets etc., which has been provided by the US Department of Justice.

2018-2022 training statistics include the following;

- 56 prosecutors and 30 prosecution investigators have been trained in relation to cryptocurrencies and darknet (investigating, search, seizure, freezing and confiscation (all of the trainings delivered by FBI and other Department of Justice employees);

- 16 prosecutors and 25 prosecution investigators were trained on parallel financial investigations, (delivered by US DOJ, ABA CEELI);

- 42 prosecutors and 16 investigators were trained on asset forfeiture and confiscation;

- 275 prosecutors and 121 investigators were trained on cybercrime and electronic evidence.

There is no information to identify whether law enforcement and judges involved in cybercrime, online fraud, online financial investigations, and electronic evidence have adopted similar training strategy.

3.4.4 **Public/Private partnerships.**

The Inter-Agency Council for the Development and Coordination of Implementation of the AML/CFT Strategy and Action Plan (AML/CFT Inter-Agency Council) is the main coordination mechanism for supervision of fulfilment of the Government’s 2014 to 2017 AML/CFT Strategy and Action Plan, as well as AML/CFT recommendations of international organisations, and coordination of activities of public agencies and self-regulatory bodies.

Whilst the formal mandate of the AML/CFT Inter-Agency Council ended in 2017, it continues to function and is chaired by the Minister of Finance. Its membership is drawn from senior officials in all AML/CFT agencies. With the adoption of the AML/CFT Law in October 2019, the AML/CFT Standing Interagency Commission will be created by this Government decision. It is planned that it will assume responsibility for development, monitoring of implementation and update of the NRA and the Action Plan. This body is yet to be established. It is envisaged that high-ranking officials from all authorities involved in the AML/CFT activities would be represented there.

The Financial Monitoring Service (FMS) is Georgia’s FIU. The FMS receives STRs and other information from obliged entities and other sources, and when there are reasonable grounds to suspect ML/TF, it sends the results of its analysis to the General Prosecutor’s Office, the Ministry of Internal Affairs, the State Security Service, and/or the Revenue Service of the Ministry of Finance for further investigation and action.

Pursuant to the AML/CFT Law, the obliged entity shall report to FMS a suspicious transaction or an attempt to prepare, conclude or carry out a suspicious transaction. In addition to a suspicious transaction, FMS through its regulation, determines the types of transactions to be reported by obliged entities to FMS.

The latest Moneval Mutual Evaluation Report underlines that the disseminations made by FMS to LEAs have been regularly used for the opening of an investigation and beginning a prosecution, however a recommendation has been given to remove any restrictions for information sharing between FMS and LEAs.

The National Bank of Georgia perform effective supervisory policies to limit the risks associated with the financial sector and exchange information related to the ML/FT with FIU based on Memorandum.

The AML Commission in the Banking Association is focused on implementation of the best international practice and high standards in struggling with money laundering and terroristic funding. The Commission closely cooperates with the National Bank of Georgia in upgrading of the regulations directed against funding of terrorists and money laundering. The Commission, by close cooperation with the National Bank of Georgia, supports assessment of an NRA. The AML Commission organises regular meetings of different local authorities with international experts, focused on rising of awareness of the society in the implications of money laundering and funding of terrorism.

In 2020, to raise awareness on reporting obligations under AML/CFT law for notaries, FMS, together with the Notary Chamber of Georgia, conducted online training for the notaries in sector.

FMS have a dedicated web page[67], which is infrequently updated with press releases (latest news is from 4th May 2021) and new typologies and indicators.

The Financial Education Division is established in National Bank of Georgia, and is tasked with the mission to raise the level of financial education among the population and promote greater awareness of financial issues in general. FinEdu[68], an independent web portal, was launched to serve this mission. This is the first Georgian educational platform that is fully dedicated to financial education and it offers educational resources such as publications and blogs, brochures, textbooks, and other similar printed and support materials, videos, and audio content.

The newly establish Digital Governance Agency[69], under the Ministry of Justice (launched July 2020) aims to provide safe, efficient "one-stop" delivery of electronic services to citizens and businesses through development of digital governance in public administration. At the same time, the agency is committed to ensure the implementation of information security policies and cyber security resilience through implementation of modern information technologies in state activities. The Digital Governance Agency administers the cyber security direction through the Government Computer Incident Rapid Response Team (CERT-GOV-GE) where all cyber incidents, according to

[67] https://www.fms.gov.ge/eng/news/

[68] https://www.finedu.gov.ge/ge/internettaghlitoba-1

[69] https://dga.gov.ge/

the Information Security Law need to be register, analyze for the public and the private sector and preventive measures need to be applied. However, there is lack of publicly available information that government CERT (cert.gov.ge) is providing some activity and cooperation with private sector.

Since 2010, a MOU between ISPs and LEA has existed. The ten largest ISPs representing the majority of the Internet industry in Georgia and the representatives of government agencies, such as Prosecution Service and the Ministry of the Interior, signed the MOU in January 2010. The Memorandum defines the principles of cooperation between ISPs and LEA in the process of investigation of cybercrime and specifies the rights as well as responsibilities of the parties. Among the most important achievements under the document is the creation of specialised contact points within the structure of ISPs and the LEA, and significant reduction of time for processing of law enforcement requests.

3.5 Republic of Moldova (Moldova)

3.5.1 Criminal landscape – national factors

Moldova has a total population of around 3 million citizens of which over 2.02 million are Internet users (68.2%). Internet growth is increasing by about 5.6% per year, whilst the use of social media has increased by 20% between 2020 and 2021 to over 1.8 million citizens. The use of credit cards by citizens in the country is very low (around 9.8%) and conducting online purchases amongst citizens is also low (around 15.4%).[70]

Moldova has adopted a new cyber-security strategy titled the Information Security Strategy of the Republic of Moldova for the years 2019-2024. The strategy identified that cybercrimes, espionage, propaganda, diversion, and excessive exploitation of personal data through ICT are the main cyber-security threats facing the government, businesses, and citizens of Moldova. The document summarises the threat of cybercrime as follows;

> *Computer fraud, computer attacks, fraud with electronic means of payment and child pornography in the global Internet network are types of crimes that require specialized investigations, appropriate training, and equipment of law enforcement bodies. Computer crime is a criminal phenomenon that, in turn, fuels many risks and crises in cyberspace, and the prevention and combating of computer crime must be a major concern of all the actors involved, especially at the institutional level, where the responsibility for developing and the application of coherent policies in the field.*[71]

The cyber-security strategy identifies some limiting factors that it aims to tackle, which include;

- No complex cyber-security audit processes;
- No studies or reports reflecting the level of cybercrime (or cyber incidents) within Moldova;
- Lack of an integrated cyber security management system;
- Lack of institutions and specialists;
- Shortage of equipment and specialised software for investigating cybercrime;
- Small service suppliers to not provide minimum cyber security of their own accord;
- ISP within Moldova are not effectively controlled by the constitutional authorities;
- The concern of intensification of external attacks and misinformation originating from the Russian Federation.

To deal with these threats and challenges, the cyber-security strategy identifies 4 pillars with a series of supporting action plans and deliverables to meet these pillars and to be concluded within the lifespan of the document;

I. Ensuring the security of the cyber-informational space and investigating cybercrime;
II. Ensuring the security of the media information space;
III. Strengthening operational capabilities;
IV. Streamlining the processes of internal coordination and international cooperation in the field of information security.

[70] https://datareportal.com/reports/digital-2021-armenia

[71] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

Historically, the AML regulatory functions of Moldova were found to be very lapse. Examples occurred in 2010-2014 where the banking system of Moldova and Latvia was used to launder US$20 Billion from the Russian Federation into Europe (called the "Global Laundromat) and in a separate banking fraud and money laundering scheme US$1 Billion was stolen (13% Moldova GDP).[72] It is reported that significant improvements have taken place since this time.

In January 2021, Moldova contributed to the global takedown of a dark web site called DarkMarket. The site had more than 20 servers in Ukraine and Moldova, which were seized during the international operation. This was a huge operation and had a significant impact upon criminals selling drugs, compromised credit card data and malware. However, it also demonstrated some capability issues where the sites were hosted in Moldova (including the region of Transnistria), and they evaded detection by national LEA and other authorities.[73]

In May 2022, the EU provided €8 million in support of cyber-security, addressing disinformation and social cohesion to Moldova. This is in response to the threats posed by the Russian Federation.[74]

In July 2022, the Coordinating Council for Information Security was created to identify the level of risk and danger for information security at National Level. Its core function is to promote and coordinate measures identified in cyber-security incidents and to propose actions to resolve these matters. Additionally, the Council's cored function is to promote and coordinate measures to implement cyber-security measures identified in the Information Security Strategy.[75]

3.5.2 Legal Framework

3.5.2.1 Cybercrime and online fraud

The Criminal Code was published in 2002 and the corresponding Budapest Convention on Cybercrime articles relating to substantive law are mainly implemented within it. There are some gaps that have been previously identified, which relate to definitions of child pornography and concepts of attempt, aiding and abetting, which are not implemented.

The Code of Procedure Code was published in 2003 and the corresponding Budapest Convention on Cybercrime articles relating to procedural law for all cybercrime investigations are implemented, albeit most provisions relating to search and seizure relate to tangible items. But broad interpretation indicates that the investigations into online fraud and electronic evidence is supported with an adequate legal framework.

[72] https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Moldova-2019.pdf

[73] https://balkaninsight.com/2021/01/13/moldovas-cyber-crime-defences-questioned-after-darknet-sting/

[74] https://fpi.ec.europa.eu/new-support-republic-moldova-cyber-security-addressing-disinformation-and-social-cohesion-2022-05-02_en

[75] https://csometer.info/updates/moldova-new-coordinating-council-information-security-created-government

3.5.2.2 **Money Laundering.**

The Criminal Code Article 243 Money Laundering deals with the conversion, transfer, concealment or disguise of illegal earnings or goods that originate from criminal ventures. The legalisation of money laundering appears to legislate for all the main offences related to individuals undertaking money laundering activities. However, there is no reference in this section to intangible property.[76]

Of relevance, the Criminal Code does not appear to reference non-tangible items such as cryptocurrencies, digital currencies, and virtual currencies. There are no definitions to indicate whether they are included in description of "property."

Whilst the Criminal Code provides significant legislation to prosecute offences of money laundering, the Criminal Procedure Code appears to provide no legal framework for the search, seizure, and confiscation beyond those available in all crimes.

It is noted that the Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) laws provide a definition of goods, which includes the following definition; "financial means, as well as funds, income, any category of corporeal or incorporeal, movable or immovable, tangible or intangible values (assets) and acts or other legal instruments in any form, including in electronic or digital form that attest a title or a right, including any share quota (interest) in respect of those values (assets);". Thus, the definition of goods includes "intangible property" in this legal text.

It is also noted that in order to introduce the necessary provisions related to virtual assets, the Office for Prevention and Fight against Money Laundering has developed the draft law for amending the AML/CFT Law, by introducing the definition of "virtual assets" and the necessary legal provisions related to the regulation and supervision of this sector.

However, there is no clear legal framework to indicate that this definition incorporates the Criminal Code (article 243) or the Criminal Procedure Code to include proceeds of crime obtained through online fraud or cybercrime in addition to those matters that are normally dealt with by the National Financial Intelligence Unit(s).

Without a meaningful description of goods or property to identify that cryptocurrencies, digital currencies and virtual currencies are covered by the Criminal Procedure Code, the search, seizure, and confiscation of criminal assets, which are represented in digital form, could be undermined.

3.5.3 **Justice response**

The Centre for Combating Cyber Crime of National Inspectorate for Investigations is the primary unit for the investigation of cybercrime. The unit has recently had several staff changes and many of the employees have only recently joined the centre.

The Prosecutor's Office has a specialised department handling all cybercrime cases.

There is no information to identify whether the entities involved in cybercrime, online fraud, online financial investigations, and electronic evidence have adopted a meaningful training strategy. These entities include law enforcement agencies, prosecutors, and judges.

[76] https://sherloc.unodc.org/cld/uploads/res/document/criminal-code-of-the-republic-of-moldova_html/Republic_of_Moldova_Criminal_Code.pdf

From 2018 the Cyber Security Centre CERT-GOV-MD undertook the role of the national CERT. It acts as the centre of computer security incidents analysis, engaged in gathering, registration and analysing the facts of all cyber security incidents that are reported to it. CERT-GOV-MD monitors the public networks to identify suspicious activities, deals with reports received from victims and deals with incidents notified to it by other CERTs.

3.5.4 **Public/Private partnerships.**

Moldova implemented a national coordination mechanism through its legislation, and this is supported by the actions taken by relevant stakeholders. The Service for Prevention and Fight of Money Laundering (SPCML) acts as the national FIU, which serves as the leading and coordination body of the AML/CFT system in Moldova. At the level of policies and programs, the cooperation is ensured by the SPCML, Government, Parliament, competent authorities, as well as specialised associations. At the operational level, the cooperation is carried out between SPCML, supervisory authorities, law enforcement, judicial and other competent authorities.

Pursuant to the approval, adoption and implementation of the NRA and its Action Plan, Government establishes, at the proposal of the SPCML, a working group for the preparation and presentation on national progress in the field of AML/CFT, to ensure the implementation of the Action Plan which has representatives from all public stakeholders and representatives of private sector (reporting entities, experts and specialists in the field of AML/CTF), when deemed necessary.

At the operational level, the cooperation between the SPCML and investigative authorities is carried out routinely, the good relations being partially explained by to the former statute of the FIU as part of the LEA. The SPCML has in place MOUs concluded with different state agencies.

Cooperation between the SPCML and the supervisory authorities takes the form of intelligence exchanges, discussions on risks and STRs, training of reporting entities and conducting joint on-site inspections. The financial supervisors notify the SPCML about any AML/CFT compliance infringement detected during their on-site or off-site supervisory actions.

During 2020, SPCML organised seminars to provide training to reporting entities for representatives of real estate agencies related to the implementation of the provisions of the AML/CFT legislation and new regulations on the application of sanctions for infringements. Also, with the support of the CLEP[77] project, a training course "Training of Trainers" for lawyers was delivered to representatives of the real estate and notary sector on the application of the provisions of the training manual in the area.

SPCML have dedicated web page which is updated regularly with press releases. From 2020 the web page has two new services, which are: high risk countries and check entities.

In the Banking Association there is separate commission of experts for the problems of AML and CTF, which is used to have permanent dialogue with the National Bank of Moldova, SPCML and other state agencies as well.

[77] Project on Controlling Corruption through Law Enforcement and Prevention (CLEP), in cooperation and assistance of the EU and CoE

For raising the awareness for online fraud and criminal money flow, several links can be found on the public web page of the National Bank of Moldova[78]. Further guidelines can be found on the government CERT website[79].

There is lack of systematic efforts and resources to raise the financial literacy, consumer protection through public-private partnership, where publications, blogs, brochures, textbooks and other similar printed and support materials, videos and audio content which could be presented to the public.

3.6 Ukraine

3.6.1 Criminal landscape – national factors

In 2021 Ukraine had a total population of around 43 million citizens of which almost 30 million were Internet users. Internet growth has increased by about 7% from 2020 to 2021, whilst the use of social media has increased by 15% to over 25.7 million citizens during the same period. The use of credit cards by citizens in the country continued to increase recording over 26% and conducting online purchases amongst citizens was increasing to around 30%.[80]

At the time of reporting at least 12 million citizens had left their homes after the invasion by Russia of which at least five million had been displaced outside the country.[81]

It is noted that the priorities of the Ukrainian authorities are centred around countering the ongoing invasion and the military response at all levels, which include cyber-security and cybercrime.

Ukraine revised its cybersecurity strategy in 2016 in the face of numerous large-scale attacks against its critical national infrastructure. The creation of the National Cybersecurity Coordination Center in 2016 and proposed updates to the legal framework to further align its legislation in accordance with the Budapest Convention on Cybercrime were two notable inclusions. The cyber-security strategy recognised increased digitalisation of services and reliance upon the Internet, which meant that responses and preparation were needed as it faced increased attacks from both DDoS attacks and zero-day malware, which was exploiting vulnerabilities in computer systems. Threat landscapes included diplomats, LEA, military and other defence actors, government infrastructure, mass media and politicians.[82]

At the time of reporting most of Ukraine is still connected to the Internet and especially in the major cities, albeit there are power outages. The communication system has proved resilient, through the support of telecom engineers and backup plans.[83]

[78] https://www.bnm.md/en/content/national-bank-calls-citizens-not-disclose-their-bank-card-details-anyone
https://www.bnm.md/en/content/recommendations-increasing-safety-use-payment-card

[79] https://stisc.gov.md/ro/constientizare

[80] https://datareportal.com/reports/digital-2021-ukraine

[81] https://www.bbc.co.uk/news/world-60555472

[82] https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/

[83] https://www.washingtonpost.com/technology/2022/03/29/ukraine-internet-faq/

From 2015, a Cyber Police Department of the National Police of Ukraine was created to handle the most serious cybercrime and online cases. In every region of Ukraine there were local cybercrime units dealing with local matters. The 100 staff in the central and local cybercrime units lead investigations into crimes relating to information security, ICT, telecom, and copyright matters. They also deal with investigations into crimes against payment systems and commercial activities.

There is recognition that the Cyber Police Departments operating at national and local levels are facing differing priorities, but the LEA and judiciary is still undertaking engagement with CPROC in pursuance of building capacity and capability in line with the Budapest Convention on Cybercrime.

Ukraine has a well-educated community, which is based on its STEM (science, technology, engineering, and mathematics) education system, which have produced talented programmers. Unfortunately, some of these entered the criminal arena. Now famous for its hacker community, Ukraine was identified as one of the top ten countries in the world to suffer cybercrime and a primary source of DDoS attacks. It is also recognised that many cybercriminals based in Ukraine are active members of darknet sites, particularly those using the Russian language.[84] However, the current situation with the ongoing invasion makes the situation pertaining to cybercrime, and other darknet based collaboration between Russian and Ukrainian criminals unclear.

In the last ten years there have been many successful law enforcement operations attempting to counter the existence of these criminal groups and it is also noted that these have continued after the invasion in 2022. Some examples include;

- January 2021 the Ukrainian Cyber Police arrested several offenders who were responsible for the creation and distribution of the Emotet malware. This malware was seen as one of the biggest threats on the Internet and allowed the offenders to undertake a variety of serious cybercrime attacks across the world. Significant assets including cash, gold and silver bars were recovered during the arrest and search;[85]
- February 2021 the Ukrainian Cyber Police arrested several suspects who were offering ransomware-as-a-service operation;[86][87]
- August 2021 the Ukrainian Cyber Police closed a network of illegal crypto-currency exchangers supporting money laundering for various individuals;[88]
- January 2022 five suspects were arrested by the Cyber Police Department using ransomware to extort money from 50 companies across the USA and Europe;[89]
- February 2022 five suspects were arrested by the Cyber Police Department allegedly using 40 phishing sites to steal credit card data from at least 70,000 people.[90]

It is not known how long the war will continue within Ukraine or even if the conflict will expand beyond the international borders. From a cyber-security perspective, a lot of information is being collected, analysed, and reported on, which relates to the cyber-attacks seen during the war. One

[84] https://ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf

[85] https://www.wired.com/story/emotet-botnet-takedown/

[86] https://www.databreachtoday.asia/suspected-egregor-ransomware-affiliates-busted-in-ukraine-a-15992

[87] https://www.youtube.com/watch?v=_BLOmClsSpc

[88] https://www.databreachtoday.asia/ukrainian-police-shutter-allegedly-illegal-crypto-exchanges-a-17287

[89] https://www.databreachtoday.asia/ukraine-police-bust-ransomware-suspects-tied-to-50-attacks-a-18302

[90] https://www.bankinfosecurity.com/5-held-in-ukraine-over-phishing-scam-70k-victims-a-18590

of the key recommendations appears the need for all countries to adopt early or refreshed cyber-security strategies that are aligned with other organisations (both public and private). Microsoft identified early lessons from the 'cyber war' that call for a coordinated and comprehensive multi-lateral and multi-stakeholder strategy to strengthen defences against a full range of cyber destructive, espionage, and influence operations in preparation for worst case scenarios.[91]

3.6.2 Legal Framework

3.6.2.1 Cybercrime and online fraud

There is a national Cyber-Security Strategy in place for Ukraine, which was published in 2016. The current situation in Ukraine poses several serious considerations for the government and its authorities in relation to cyber-security rendering parts of the current strategy out of date and/or redundant. At an appropriate time, the national cyber-security strategy can be reviewed, updated, and published, but it is recognised that the priorities for this document are lessoned in the face of the ongoing conflict.

Previous reviews of the legal framework of Ukraine have identified that it has legislation in its criminal code that meet most of the requirements of the Budapest Convention on Cybercrime Comments relevant to online fraud indicate that there is no obvious differentiation between online fraud and other types of fraud cited in the legal framework. Previous comments provided to Ukraine include missing elements of some definitions relating to cybercrime and electronic evidence remain. [92]

Similar reviews of the criminal procedure code of Ukraine have identified a few missing definitions when compared to the articles in the Budapest Convention on Cybercrime. Definitions for electronic evidence and traffic data are not present. There are other apparent gaps in legislation related to preservation orders (Art 18 BCC), production orders (Art 15 BCC) and search and seizure of computer data (Art 19 BCC).[93]

3.6.2.2 Money Laundering.

Article 209, Legalisation (laundering) of criminally obtained money and other property - provides a criminal offence relating to effecting financial transactions and other deals involving money or other property known to be proceeds of crime.

[91] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[92] https://www.coe.int/en/web/octopus/-/ukraine?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_HWAFAbhgD3hQ&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

[93] https://www.coe.int/en/web/octopus/-/ukraine?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_HWAFAbhgD3hQ&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

The Criminal Code does not seem to include references to intangible items such as cryptocurrencies, digital currencies, and virtual currencies. There are no definitions to indicate whether they are included in description of "money or other property."

The Criminal Procedure Code, Articles 100, 160-166 and 170-174 deal with special confiscation, and provide a framework for the investigation, search, seizure and confiscation of funds or other assets in relation to money laundering. However, there is no meaningful description of funds or other assets to identify that cryptocurrencies, digital currencies and virtual currencies are included in the CPC. If these are not included in any definition, the search, seizure, and confiscation of criminal assets, which are represented in digital form, could be undermined.

3.6.3 **Criminal justice response**

Following a reform in 2015 there were 100 officers trained and assigned to cybercrime units. 27 operatives were based at the Cyber Police Department in Kyiv dealing with national and international cybercrime investigations. The remainder were allocated to local cybercrime units dealing with regional cybercrime matters.

The department has a high level of competency and can investigate all crimes committed by means of ICT. Such crimes include online fraud, other crimes against CIA, child abuse and copyright offences. Investigators within the Cyber Police Department lead criminal proceedings on such matters.

The Forensic Science Service of the Ministry of Interior provides expertise in the digital forensic examination of digital devices for court processes.

The Department of Counterintelligence Protection of State's interests is another specialised LEA within Ukraine. This is part of the national security services and undertakes investigations related to the CIA of computer and telecom networks.

A dedicated administrative financial intelligence unit called The State Financial Monitoring Service of Ukraine exists, within the structure of the Ministry of Finance.

CERT-UA fulfils the role of the national CERT. It provides support through the collation and analysis of computer incidents, sharing information and acting as a contact point for users needing assistance.

There is no information to identify whether the entities involved in cybercrime, online fraud, online financial investigations, and electronic evidence have adopted a meaningful training strategy. These entities include law enforcement agencies, prosecutors, and judges.

3.6.4 **Public private cooperation.**

The State Financial Monitoring Service (SFMS) fulfils the role of national FIU, and it generates financial intelligence of a high order. Spontaneous case referrals regularly trigger investigations into ML, associated predicate offences or FT. LEAs also seek intelligence from the SFMS on a regular basis to support their investigative efforts. Cooperation at operational level and information exchange between authorities is generally positive, particularly where the SFMS is involved.

The SFMS produces good quality operational analysis. An effective mechanism allows for the proactive collection, risk-based prioritisation and analysis of financial intelligence originating from a broad range of sources, including the very high number of reports, mainly mandatory, and filed by the obliged entities. Reporting appears to be in line with Ukraine's risk profile, that resulted in a significant number of case referral to LEAs.

The private sector appears to have a positive and constructive relationship with both the SFMS and with their respective regulators, communication and education came out as being strengths of this relationship. The private sector's understanding of their AML/CFT obligations was demonstrably very good. However, outside of the banking sector, the understanding of the ML/TF risks facing those businesses was much weaker.

Very significant efforts have been made by the National Bank of Ukraine in relation to ensuring transparency of beneficial ownership of banks and in removing criminals from control of banks. The National Bank of Ukraine (NBU) has a good understanding of risk and applies an adequate risk-based approach to the supervision of banks. Other supervisors had a basic understanding of risks or understanding was lacking, which mean that cooperation and training is needed to fill the gaps.

In 2021, the SFMS promoted the activities of the Public Council within its organisation to improve the mechanisms of interaction between the SFMS and the public. In 2021, the Public Council at the SFMS held two meetings in the video conference format, where the members of the Council were informed about the implementation by the SFMS of the AML/CFT policy. The materials of the meetings and press releases are posted on the dedicated SFMS website. In 2021, within the framework of interaction with the public, the SFMS has organized;

- participation of the public representatives in the international scientific AML/CFT workshops;
- publishing over 450 information notifications on financial monitoring on the SFMS's official website;

During 2021, the SFMS representatives took part in 56 educational events organized by the Academy of Financial Monitoring, which were attended by 2035 listeners. During 2021, the SFMS representatives took part in 83 educational events held for 4378 persons.

In 2021, the Academy of Financial Monitoring trained 1,878 listeners, including;

- 665 specialists - representatives of law enforcement, intelligence, judicial and other state authorities;
- 1213 specialists – compliant officers of reporting entities from the private sector.

In the banking association there is a special committee for compliance and financial monitoring, which is used to hold permanent dialogue with the National Bank of Ukraine and SFMS.

On 14 February 2022, National Bank conducted the All-Ukrainian information campaign on payment security #FraudGoodbye together with the Cyber Police Department of the National Police of Ukraine, and with the support of:

- International Finance Corporation (IFC) in partnership with the Swiss State Secretariat for Economic Affairs (SECO) and the Great Britain Foundation for Effective Governance;
- Ministry of Digital Transformation of Ukraine.

The purpose of the campaign was to improve citizens' awareness of cyber hygiene and to promote the formation of a culture of safe behaviour in the virtual space, as well as to remind about the basic rules for the security of non-cash payments.

There is lack of information that government CERT team (cert.gov.ua) is providing any current activity or cooperation with the private sector.

4 Standard mechanisms for preventing and combatting online fraud and criminal money flows with emphasis of some practices in the region.

Fraud is generally considered a predicate crime, the proceeds of which can then be laundered. In some examples the divide is less clear, such as act of being a 'money mule', which can be considered both an act of money laundering and a fraud against the financial institution at the same time. The money mule may have committed fraud in the setting up of the account and the act of money laundering through the account may constitute a fraud if activity has been accompanied with false documentation to the financial institution. Money laundering, more broadly, may require a criminal party to make fraudulent claims, misrepresent facts or misuse of a facility of the financial institutions.

Successful prevention, detection, and investigation of cybercrime, proceeds from online crime and money laundering requires the inclusion of a wide range of stakeholders, and in particular it requires the involvement of financial institutions and other obliged entities under the AML and CFT legislation, financial intelligence units (FIUs), AML/CFT regulatory and supervisory bodies, cybercrime units, financial investigation units, and prosecution services. Though this criminality can be significantly reduced by raising awareness among the potential victims, its prevention and detection also heavily depends on the readiness of obliged entities to mitigate the risks associated with these offences and their ability to recognise the suspicious patterns related to their clients, products, services, and transactions. These preventive and detective measures may serve as good practices and could become elements of more systematic future approaches and strategies that are aimed at the prevention of money laundering and the financing of terrorism, and at the search, seizure, and confiscation of proceeds from crime on the Internet.

4.1 Mechanism for reporting on online fraud and criminal money flow

Timely and efficient reporting about online fraud and cybercrime to the relevant authorities and ensuring meaningful follow-up of the crime reports through the financial intelligence and criminal justice system, as well as through financial investigation is one of the most important measures against offences, which involve computer systems and data and their proceeds.

4.1.1 Unified Reporting Center or National Fraud Database

In the countries of the Eastern Partnership region there is fragmentation of the reporting for the online fraud which varies across responsible institutions. In some instances, a contact form needs to be fulfilled in other it is document that needs to be downloaded, filled, and sent to specific email address. Either individuals who suffered the fraud are not reporting or they are reporting the same fraud in several platforms through institutions and rarely receive feedback.

In response to the underreporting[94] of online fraud and more general cybercrime, governments and non-governmental organizations have implemented initiatives designed to increase reporting

[94] Underreporting of fraudulent activity can be due to institutional embarrassment, other reputational concerns, or lack of actionable intelligence to share with law enforcement.

by streamlining the cybercrime reporting process. This process depending on the type of cybercrime committed can normally involve numerous agencies depending on the type of cybercrime committed, through websites or hotlines. (e.g. online financial fraud can involve police, banks, and other financial institutions, as well as government agencies involved in the investigation of financial cybercrimes). This means that number of reported fraud and other forms of cybercrime is scattered in different platforms and under the different agencies, which are constantly lacking the capabilities to analyse new Internet frauds or follow the related proceeds.

A unified online reporting platform allows LEA to detect not only individual offences but to identify trends and to analyse Internet-related crime in a more comprehensive manner and implement adequate strategies. Once online reporting is widely used there will be an increase in reports which will be not related only to crimes, but to disputes or intelligence. Implementing methods to filter reports will be important along with the ability for crimes reports to be gathered centrally and to be linked. The creation of an online resource for reporting fraud and other forms of online crime may also be a resource for alerting the public of types of crime being committed in a country, and against which the public may be able to adopt prevention measures.

In addition, this type of resource may also be used to disseminate similar information that may be available from other players such as banks, CERT's and others affected by cybercrime. Having a "one stop" resource is much more likely to be seen as valuable by citizens, rather than having separate sector resources. However, to succeed there must be ***trust*** between all stakeholders, secure storage of data in centralised database and encrypted flow of information in both directions.

- Some good examples and practices related to the fraud and other forms of Internet crime are; Internet Crime Complaint Center;[95]
- ActionFraud - National Fraud & Cyber Crime Reporting Center;[96]
- Europol Reporting Center.[97]

4.1.2 Reports on Suspicious Transaction Reports[98] from the reporting entities regarding AML/CFT

Recommendation 20 of FATF standard is demanding: If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity[99], or are related to terrorist financing, it is required to report promptly its suspicions to the financial intelligence unit (FIU). To comply with its requirements under R.20, the private sector must collect and share personally identifiable information with the FIU. The private sector is also required to identify and verify the identity of customers and undertake ongoing monitoring of their

[95] https://www.ic3.gov/Home/FileComplaint

[96] https://www.actionfraud.police.uk/

[97] https://www.europol.europa.eu/report-a-crime

[98] A Suspicious Transaction Report (STR) is a document that financial institutions must file with their Financial Intelligence Unit (FIU) whenever there is a suspected case of money laundering or fraud. These reports are tools to help monitor any activity within finance-related industries that is deemed out of the ordinary, a precursor of illegal activity, or might threaten public safety.

[99] refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence

transactions/circumstances to ensure that their activities are in line with what they have reported and to have a basis on which to determine if their transactions may be suspicious. The private sector uses transaction monitoring systems, including common risk indicators (such as those provided by the FATF, government authorities or commercial providers) to identify potential suspicious activity across a range of crime types.

In Eastern Partnership region almost all STR are submitted by banks as they have dominant market share in the financial system. STR are submitted according to a process of detailed risk indicators related to the type of financial transaction product, client, geolocation and many more. Banks maybe underreporting STRs since they have overreliance on typologies and red flag indicators issued by FIU, and they need to improve with additional quantitative and qualitative indicators. Nonetheless, in one of the countries in Eastern Partnership region STRs contributed to the discovery of the two biggest ML cases[100] and led to multiple successful ML investigations and prosecutions.

Through the analysis of the latest MONEYVAL mutual evaluation reports (MER) on each of the countries in the region significant findings, which are related to the STR are as follows;

- Most of the countries are compliant with Recommendation 20 for reporting of suspicious transaction, with guidance on suspicious transactions or business relations and guidance on typologies publish by the FIU based on the national experience;
- In most of the countries of the region the number of defensive STR have a downturn trend or the amount of big number low quality STR is lowering, which means that quality of the submitted STR to the FIU is more useful;
- Less awareness and reporting of STR or no STRs submitted by other non-financial entity (DNFBP[101]), which means further training and awareness raising initiatives must be put by the FIU to increase the reporting.

4.1.3 Using a common data format and privacy technologies for the reporting database

Data relevant to cybercrime investigations is often voluminous, scattered across different jurisdictions and venues, and archived in disparate file formats that obstruct machine-based sharing and processing. To overcome this problem, there are some efforts[102] to develop common data format for the exchange of data related to the technical aspects of phishing, fraud, and other forms of electronic crime.

Some newer initiatives, which are led by private sector with the intention to comply with strict AML regulation, can rely on innovation and technological advancement in the field of Artificial Intelligence with privacy preserving analytics and privacy enhancing technologies[103] to limit exposure of information and maximise analytical or computational processes to detect fraudulent activity from different reporting databases. (More details in chapter 4.6.5 private-private

[100] Moldova - "Banking Fraud" and the "Global Laundromat"

[101] DNFBP stands for Designated Non-Financial Businesses and Professions

[102] Anti-Phishing Working Group (APWG) developed an Incident Object Description Exchange Format (IODEF-XML-based scheme)

[103] Future of Financial Intelligence Sharing (FFIS) Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime (January, 2021)
https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf

information sharing). Common collaborative platforms facilitate data sharing between public and private sector institutions, joint private investigations and may permit more automated mechanisms for detection of fraud patterns and related criminal money flow in the future.

4.2 Prevention and public awareness

Public education and awareness and other measures are essential elements to prevent online fraud, other forms of financial crime, and criminal money flows on the Internet. The offer in this respect is increasing, ranging from public websites with general fraud prevention information or materials and educational materials and courses, to recommendations for employees of public or private sector organisations or specific resources to prevent risks in a specific sector, or assistance to victims of fraud.

It is important that prevention and public awareness initiatives dealing with online fraud, present a united front as far as possible, and to avoid mixed messaging that may occur if strategies are developed at the individual domestic level.

Public education and awareness are essential elements to prevent online fraud and other forms of crime. There are increasing number of public websites with;

- General fraud prevention information;
- Consumer education and protection information;
- Basic Cyber Hygiene[104] practices for the individuals and small companies;
- Educational materials and courses;
- Specific resources to prevent risks in a specific sector;
- Assistance to victims of fraud.

Experience from the countries from the region on raising public awareness vary. Developing financial education platforms where public can be informed about different online frauds is still in progress. Lots of information in the forms of publication, blogs, brochures, infographics, and short videos need to be presented to explain the online fraud threats and to identify to the public, role of the money mules and potential consequences.

More effort is needed in the region for raising such awareness, to promote financial literacy and changes to people’s behaviour, especially as the use of the Internet, online payment services and differing applications continue to expand in the region.

4.3 Risk management measures for prevention and control of online fraud and criminal money flow

Every country is obliged to implement risk-based approach, which means to take a more focussed approach in areas where high risks remain, or implementation could be enhanced. Countries should first identify, assess, and understand the risk of ML and TF that they are exposed to and then adopt appropriate measures to mitigate the risks. This enables each country to apply a more

[104] Cybersecurity Awareness Month, every year in October, is a collaboration between government and private industry to raise awareness about cybersecurity and empower everyone to protect their personal data from cybercrime.

flexible set of measures to target their resources more effectively and apply measures proportionate to the nature of risk.

4.3.1 Risk management, know your customer (KYC) and customer due diligence (CDD) measures

Financial institutions, through regulation, are obliged to design and implement appropriate measures and controls to mitigate the potential money laundering risks in respect of the relevant products, services, or customers, based on a thorough risk assessment process. Such measures and controls may require investments in terms of resources and time to identify and capture appropriate risk data.

With specific emphasise on the online fraud and criminal flows, such measures and controls may include;

- Increased awareness by the institution of higher risk situations determined by types of financial services and/or products and/or customers;
- Appropriate levels of know your customer ("KYC") or enhanced due diligence;
- Escalation for approval of the establishment of an account or relationship;
- Record-keeping;
- Increased monitoring of transactions;
- Increased levels of on-going controls and reviews of relationships.

4.3.2 Preventive measures to combat online fraud activity

For the effective identification of the suspicious transactions, FIU develop risk indicators and specific guidelines for different sectors. In addition to the indicators, additional measures can further minimise the risks from online fraud. Recommendations for risk indicators depend a lot on the regulation[105] applied for the financial institution in each country.

Because fraudsters change their modus operandi, the signals for fraud also change. The amounts paid, type of payee account, and profile of customer will be different for a fraud that is leveraging a personal relationship such as a romance fraud compared to those for an investment fraud. These variables constantly change, and sufficient flexibility is required in how the rules that manage risk can be authored and adapted dynamically once the characteristics of a new fraud type are identified.

If introducing new fraud rules is a difficult and time-consuming effort for a bank, then fraud can go unmanaged for longer, losses escalate and fraudsters realising they have uncovered a weak spot, can increase their rate of attack.

Some of the measures that financial sector can apply to detect and manage these risks, are listed at Annex A below.

[105] Regulation on payment security and general IT&cyber security in the financial sector

However, one of the most effective measures to implement to combat online fraud is that financial institutions need to establish processes including to cool-off or delay mechanism[106] where transactions have a high-risk score[107] related to online fraud or criminal money flow.

4.3.3 Postpone transaction and seize and confiscate criminal proceeds

4.3.3.1 Postpone the transaction

The Warsaw Convention provides standards for the postponement of transactions. Article 14 requires parties to take measures to permit urgent action to be taken by FIUs or, if appropriate, other competent authorities or bodies, to postpone a domestic suspicious transaction. National law shall determine the duration of such measures.

In most countries, the decision to postpone a transaction is based on certain indicators, even if they are not included in a formal document;

- The transaction is assessed as highly unusual or suspicious, based on indicators (possible detection of online fraud or criminal money flow);
- Checks in various databases or other sources indicate that the person(s) involved in transactions may be/are related to criminals (possible criminal money flow);
- There is a danger that the execution of the transaction may hamper or substantially impede the seizure of proceeds of criminal activity.

The average duration of the postponement of the suspected transaction by the FIU is *72 hours*. However, this differs across the region, and if more time is required for in-depth analysis, FIU can prolong this period.

With the latest thematic review[108] on Article 14 of the Warsaw convention, these are the conclusion for the countries from the Eastern Partnership region;

- The Armenian AML/CFT law provides that the authorised body may suspend a suspicious transaction or business relationship, possibly relating to ML or TF, for up to five days;
- The Azerbaijan FIU is permitted to suspend suspicious transactions, for a maximum duration of two business days and 72 hours additionally;
- The Georgian AML/CFT law, provides that the authorised body may suspend a suspicious transaction or business relationship, possibly relating to ML or TF, for up 72 hours. Inconsistent information about possibilities of the authority[109] in Georgia to prevent timely

[106] In some cases, just a telephone conversation with the client about high possibility of fraud can stop the payment to finish at fraudster account. Financial institution can implement process of IBAN change of trusted beneficiary, which can be used as a delay of the payment execution.

[107] See Annex A on how to compute transaction risk score.

[108] Thematic Monitoring Review of the Conference of the Parties to CETS No.198 on Article 14 ("Postponement of domestic suspicious transactions"), Strasbourg 28 October 2020

[109] In the latest Georgia MONEYVAL MER there is issue related :

"This was subject to one issue concerning transfers from bank accounts after an STR has been made. The LEAs identified several cases where, by the time a freezing order on a bank account was in place, the assets had already been transferred, often out of the jurisdiction. Inconsistent information about the reasons for this was provided to the assessment team.

- According to representatives from the banking sector, banks wait for 3 days after making an STR before carrying out a request to transfer funds.

dissipation of the assets gathered through online fraud through the traditional banking system indicates that this aspect of the system needs to be further examined urgently and practices revised;

- The Moldovan FIU is permitted to suspend suspicious transactions, for a maximum duration of thirty working days;
- The Ukrainian FIU has the power to postpone domestic suspicious transactions for a maximum duration of thirty working days.

4.3.3.2 **Seize and Confiscate**

Recommendation 4 of FATF Standards requires countries to adopt measures like those set out in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties;

a. property laundered;
b. Proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences;
c. Property that is the proceeds of, or used in, or intended or allocated for use in, the financing of Terrorism, terrorist acts or terrorist organisations;
d. Property of corresponding value.

These measures should include the authority to;

a. Identify, trace, and evaluate property that is subject to confiscation;
b. Carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer, or disposal of such property;
c. Take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation;
d. Take any appropriate investigative measures.

In the latest MER, Moldova is assessed by MONEYVAL evaluators as compliant (C) and other project countries are largely compliant with Recommendation 4, which means that current practices from this country can serve as guide for the other countries in the region.

The main findings for the countries in the region are that number of confiscations ordered in respect of predicate crimes (e.g. online fraud) is low and may indicate that these measures are not used as central tool for combating predicate offences. Furthermore, there is no central management of seized property, nor are personel fully equipped and trained to deal properly with all types of property that may be seized or confiscated.

4.4 Harmonised legal framework based on international standards

One of the key objectives in the investigation of online fraud is the recovery of losses for the victims and countering money laundering. To properly enable this, parallel financial investigations supported by legal frameworks are necessary. The creation of a legal framework for the

- According to the FMS, it always notifies the GPO about STRs in sufficient time to allow an emergency freezing order to be obtained within the 3–day window before funds is transferred.
- According to the GPO, apart from cases where there might be an operational need to allow funds to be moved, emergency freezing measures are applied, whenever necessary, immediately after receiving an STR. "

criminalization of conduct related to criminal money flows on the Internet, for the effective investigation of cybercrime, money laundering and the financing of terrorism, for financial investigations and the confiscation of crime proceeds and for international cooperation is therefore essential.

The Budapest Convention on Cybercrime assisted countries to meet the challenge of investigation of cybercrime and online fraud. All countries in the region have adopted the Budapest Convention on Cybercrime, but some still need to improve legal frameworks as described above. Lately the Convention is complemented by Second additional protocol on enhanced co-operation and disclosure of electronic evidence CETS 224 (of 2022).

The Warsaw Conventions and FATF International standards on combating money laundering and the financing of terrorism & proliferation give more focused approach in investigating ML and terrorism. All countries in the Eastern Partnership project have adopted the Warsaw Convention, but improvements are necessary, especially to further strengthen the legislation and application that will allow proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction-based confiscation)[110].

FATF issued a set of recommendation, which can serve as guidance to set up adequate controls based on the national risk assessment. Implementation of this framework is assessed through Mutual Evaluation processes[111], and through the assessment processes of the International Monetary Fund and the World Bank – based on the FATF's common assessment methodology. Countries in Eastern Partnership region are regularly monitored and assessed on their fulfilment and implementation of the FATF standards.

4.5 Develop adequate skills, resources, and interagency co-operation

4.5.1 New skills and resources

To prevent and control online fraud related to new products, new business practices, new delivery mechanisms, and use of new and developing technology,[112] adequate skills and resources should be implemented by all relevant stakeholders. These advances should be carefully planned and developed.

One of the key components in early detection of online fraud is using the OSINT techniques. OSINT is key to horizon scanning, especially early warning either expert driven in partnerships or automatically data driven. OSINT is giving opportunities for national competent authorities to monitor social networks, communication channels, marketplaces, or fake sites of the legitimate company to identify online fraud or de-anonymize an actor. Fraudsters and criminal groups distribute announcements through various sources (social networks, emails, announcements, etc.) and it is crucial for the LEA and FIU to identify such online activity on time.

[110] Offenders must demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

[111] The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) is an independent monitoring body entrusted by the Committee of Ministers of the Council of Europe with the task of assessing compliance with the principal standards to counter money laundering and terrorist financing (AML/CFT) and the effectiveness of their implementation.

[112] FATF Recommendation 15

Another imperative is to set up specialised units to conduct proper cryptocurrency analysis using blockchain analytics tooling to track criminal money flows. It is especially of interest to track transactions from payments supporting illegal transactions and orders to VASP[113]. Some resources like blockchain analytics solutions have implemented assets tracking and understanding of the flow with intelligence obtained through crypto-dusting[114] and by sharing TagPacks[115].

The LEA should allocate adequate skills and resources to seize cryptocurrency that derive from illicit activity. Although significant steps have been made at national level to increase the financial analytical capacity of LEAs, there is still a great need for such experts in police forces and prosecution services. The pseudo-anonymity, which characterised cryptocurrency, and the technical complexity of the use of modern and emerging electronic technologies, which require a high level of technical knowledge and cross-border cooperation to achieve a successful investigation, constitute additional challenges for LEAs.

Another challenge for the National FIUs is to embrace the innovation in digitalisation and digital transformation[116], to be able to process and analyse large quantities of unstructured data from increasing number of reporting entities, sectors, and transactions to timely detect and disrupt ML transactions. This means building advanced analytics team(s), whether internal or outsourced, providing sufficient resources covering initial development, ongoing operational and maintenance costs of Advanced Analytical Tool, and providing training opportunities for relevant personnel.

Training on new types of online fraud, cybercrime, new threats, trends, typologies, technology, international standards for the different stakeholders of investigating, prosecuting, and adjudicating cyber offences is required by many countries. Certain organisational initiatives have been launched[117] to support law enforcement although concepts, guidelines have been elaborated to further increase the importance of training as well as to support national authorities with elaborating training strategies. There are on-going initiatives of the Council of Europe supporting national authorities in the cooperation against cybercrime[118].

4.5.2 **Inter-agency co-operation**

Cooperation between authorities responsible for financial investigations and confiscation of proceeds, measures against money laundering and cybercrime is considered an important condition for success against criminal money on the Internet.

[113] VASP is Virtual Asset Service Provider or Crypto-Exchange

[114] Police shall adapt their covert operating procedures to be able to send small amounts of Bitcoin to suspicious addresses and then follow the track.

[115] TagPacks are a method and format defined by a consortium of partners (including INTERPOL). They enable investigators' sharing of intelligence.

[116] FATF DIGITAL TRANSFORMATION OF AML/CFT FOR OPERATIONAL AGENCIES DETECTION OF SUSPICIOUS ACTIVITIES AND ANALYSIS OF FINANCIAL INTELLIGENCE, October 2021

[117]ECTEG - http://www.ecteg.eu/; University College Dublin Centre for Cybercrime Investigations - https://www.ucd.ie/cci/; European Union Agency for Law Enforcement Training CEPOL https://www.cepol.europa.eu/

[118]https://www.coe.int/en/web/cybercrime

Within Recommendation 2 of the revised FATF Recommendations, there is an essential criterion requiring jurisdictions to ensure mechanisms to enable policy makers, the FIUs, LEA, supervisors, and other relevant competent authorities to co-operate, and where appropriate, co-ordinate domestically with each other concerning the development and implementation of AML/CFT policies and activities. Such mechanisms should apply at both policymaking and operational levels. Thus, the JIT (operational co-operation) are now a part of the international standard in the AML/CFT area.

According to the last MONEYVAL evaluation report of the countries from the Eastern Partnership region, they are largely compliant (LC)[119] with Recommendation 2, which mean that they have established good mechanisms for policy making[120] and on operational level through bilateral MOU by the FIU with other relevant and competent authority. Also, cooperation between the FIU and the supervisors is at an adequate level to allow rapid exchange of information and best practices.

AML Cooperation between the FIU, as the main source of intelligence for AML/CFT purposes, and other law enforcement authorities, is a strong point in the system. Information is exchanged rapidly and securely between the relevant authorities spontaneously and upon request. In latest Armenia and Georgia evaluations, findings identified limitations on the ability of the LEA to routinely request information held by the financial institutions or financial intelligence from the FIU respectively, which can have negative impact on inter-agency cooperation to combat with online fraud as predicate offence.

An additional finding in Armenia is that the LEA have difficulties in turning financial intelligence into evidence, which underlines the need for more training of LEAs on investigative matters. Some effort is required to be paid in continuous and consistent multilateral cooperation and coordination mechanism dedicated to problem identification at AML/CFT system level and the adoption of proactive or reactive policies to cope with new emerging issues.

4.6 Public-private co-operation and information exchange

Public-private co-operation and information exchange is arguably the measure with the strongest impact on the prevention and control of criminal money flows on the Internet. It addresses a key problem, namely the limited sharing and use of existing information between domestic financial institutions, and between financial institutions and LEA.

4.6.1 **Public-private co-operation**

There are no specialised prosecution units dealing with cybercrime investigations in the legal systems of the Eastern Partnership, which decreases their role and interest in the development of public-private cooperation opportunities. LEA in the Eastern Partnership states are most active

[119] There are four possible levels of technical compliance: compliant (C), largely compliant (LC), partially compliant (PC),and non-compliant (NC).

[120] In line with the recently adopted AML/CFT Law, Georgia plan to substitute AML/CFT Inter-Agency Council (mandate terminated formally at the end of 2017 but remained functional) and establish new body AML/CFT Standing Interagency Commission. Coordination of the efforts of various crime, including ML was conducted primarily based on the 2017-2021 Prosecutor Strategy.

and common representatives of the state in the process of public-private cooperation against cybercrime.

Most commonly, the cybercrime/high-tech/computer crime units at the national police forces are the primary source of requests for access to data, as these units are most specialised in handling of electronic evidence in criminal cases. In some states of the Eastern Partnership, Investigative Committees as central authorities of investigation separate from police forces are handling the cases. The investigative units also rely very often on either internal or external expert capacity in both securing and processing electronic evidence.

Enhanced public-private co-operation and information exchange at the national, regional, and international level is desirable.

In terms of public-private cooperation it may be noted that national CERT teams are quite active in this area. Many have been set up either within the government working groups or committees to work with representatives from the private sector or experts in the field of AML/CFT. Working groups and committees have a specific mandate to work on some topics or to follow the implementation on some action plan through different institutions.

Another factor in the public-private cooperation can be seen in the form of banking associations as expert committee where various member are having discussions regarding the compliance with the requirements of AML and compliance legislation, recommendations of Financial Action Task Force (FATF) and requirements of FIU and members to exchange experience and explore new ways to cooperate in this field. *These committees can be seen as useful tools to discuss new typologies related to the new online frauds and criminal flows and to further discuss about private-private information sharing. No private-public information sharing initiatives and/or platforms have been identified in the Eastern Partnership region.*

Another area that requires attention is the exchange of data between the public and private sectors, and the exchange of security/CERT related data with LEA. Traditionally the CERT community uses relatively informal ways of sharing information and the TLP (traffic light protocol) to limit distribution of data. With CERT bodies increasingly being incorporated in security services and regulators that have close ties to law enforcement (as it is the case in almost all the EAP states where the government CERT acts as a national CERT), the question as to the status and legality of this exchange arises. This is an area where good practices would be invaluable, not only for the EAP region, but for the global security and law enforcement communities.

4.6.2 Data protection authorities

The data protection authorities are becoming increasingly important factor in the public-private cooperation and information sharing for two primary reasons:

- the mass processing of personal data through data retention regulations and practices that need oversight;
- law enforcement access to such data needs to comply with data protection principles.

All Eastern partnership countries have both a data protection act and an authority that oversees and enforces the legislation. The institutional frameworks are different, as Moldova and Georgia have independent authorities, while in Armenia, Azerbaijan, and Ukraine undertake these functions within various Ministries or an Ombudsman's Office.

Data processing can be perceived by some countries as a blocking factor that makes public private cooperation and information exchange less easy, if not impossible, due to the lack of grounds for processing the data involved. In general, privacy should not be a concern if there are fair and legitimate grounds for processing. This could be attributed to the lack of meaningful dialogue and sharing of common values between the law enforcement community and the data protection community, which leads to the need for more guidance on how to achieve efficient public - private cooperation and information sharing.

4.6.3 **Memoranda of cooperation LEA with the ISP**

MOU are concluded in Armenia and Georgia between the law enforcement and the Internet service providers industry - with varying degree of coverage as regards the law enforcement representatives. Such cooperation agreements have not been seen yet as decisive factors in day-to-day cooperation and more weight is given to the clear and balanced legislative background as a primary source for such cooperation.

4.6.4 **Cybersecurity initiatives**

There is global agreement for increasing cyber-security and need for a national cyber-security strategy is recognised by most countries in the region as a sound response. Most are either working on such a strategy or have already adopted one.

The process of identifying CNI and legislation that implements security standards for infrastructure to be adequate is already underway in the region. Generally, countries that have adopted a cybersecurity strategy have not always specified cybercrime as an action plan or risk factor. This may lead to functional separation of the security function from the law enforcement function and could have the altogether undesirable effect that online fraud is reported to one type of authority but does not reach the other (see part 4.1.1 Unified Reporting Center or National Fraud Database).

In many cases investigators will have to cooperate with industry cybersecurity experts or crypto analysts to identify the malicious actors, analyse the complex flow of the transaction data, protect the electronic evidence, and build better resilience from such future attacks and frauds.

4.6.5 **Private-private information sharing**

Single regulated entity's understanding of risk will be limited by their siloed view of relevant threats. An ability to analyse networked data derived from multiple financial institutions will have a higher efficacy in detecting risk that spans multiple institutions. However, there are a range of complex policy[121] considerations relevant to the growth of private-private information sharing in the AML/CFT space.

[121] The Netherlands 2019 "Joint Action Plan" on the prevention of money laundering (transaction monitoring and post suspicion private-private sharing); 2019-2022 UK Economic Crime Plan (pre-suspicion and post-suspicion private-private sharing); US 2021 AML Act and prescribed growth of FinCEN Innovation programme;

Within the AML/CFT framework, the traditional conception of the FIU is that it is the public agency responsible for undertaking analysis of all suspicious reports and providing associated intelligence support to operational agencies. However, resource constraints severely limit the ability for FIUs to process the reporting it receives. FIUs do not have a live picture of transactions and only operate with the segment of financial behaviour that is observable through a formal filed report(s).

In contrast to relying on FIU analysis to 'connect the dots' from filed reports, private-private sharing offers:
The opportunity for a real time understanding of financial behaviour;
The potential for network wide analytics that capture the complete behaviour of an entity across multiple regulated entities;

- Working from comprehensive data, which is searchable at source, rather than a partial record of historic transactions;
- If coordinated, the potential for more resources – collectively, in terms of investigating staff and technology – to be applied to support analysis within major regulated entities compared to FIUs.

The international standards regime, established through FATF, does not currently provide clear support or direction in terms of the need to establish legal gateways for regulated entities to share AML/CFT risk information between one another. However, in a major contribution to advancing the international standards engagement with private-private information sharing, in July 2021, FATF - the international standards setter for the AML/CFT regime - published a "Stocktake on Data Pooling, Collaborative Analytics and Data Protection"[122]. The study examined how different jurisdictions and initiatives had supported technologies that allow collaborative analytics between financial institutions and other entities, while respecting national and international data privacy and protection legal frameworks. According to FATF, "data pooling and collaborative analytics can help financial institutions understand better, assess, and mitigate money laundering and terrorist financing risks. This will make it easier, more dynamic, effective, and efficient to identify these activities. It can reduce the number of false positives, enabling the private sector to comply in a timelier and less burdensome manner."

FATF go on to state that "Data sharing is critical to fight money laundering and the financing of terrorism and proliferation. Multinational criminal schemes do not respect national boundaries, nor do criminals or terrorists only exploit one institution to launder their ill-gotten gains or move or use funds with links to terrorism. Customers are increasingly using multiple institutions for banking, instead of banking with a single financial institution with a large market share. This means that data about individual customers is becoming increasingly dispersed across a wide array of financial institutions. If multiple financial institutions share data and apply advanced analytics, it can reveal trends or potentially suspicious activities that could otherwise go undetected by a sole institution."

Monetary Authority of Singapore Consultation Paper on "FI-FI Information Sharing Platform for AML/CFT" October 2021

[122] https://www.fatf-gafi.org/media/fatf/documents/Stocktake-Datapooling-Collaborative-Analytics.pdf

There are number of new private information sharing initiatives[123] and studies[124] that explain the pros and cons of such integrated platform approach. The study is pointing out that these initiatives can be supported by being encompassed with a shared strategic vision between public and private stakeholders; delivered through a clear enabling legislative and regulatory environment; and developed with a framework of good governance, data ethics and accountability.

Through private-private collaboration platforms, it is possible to achieve more consistent *financial exclusion decisions against fraudsters and high-risk entities*. It is possible to support real-time identification and interdiction of the proceeds of crime flowing across multiple financial institutions – and even across borders. It is possible to re-orient the AML framework from being focused on collecting a vast record of historic suspicious transactions, to being an intelligence-led public-private and private-private collaborative effort to dismantle crime networks. (See Annex B)

These new initiatives need to be discussed further in countries from the Eastern Partnership region with public initiative and support, together with experts from the private sector (ex. Banking association committee on AML or other working groups) to exchange experience and explore new ways to cooperate in this field.

[123] 1. Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) 2. Insurance Fraud Bureau 3. National SIRA – Synectics Solutions35 4. UK Finance Fraud Intelligence Sharing Service (FISS)36 5. UK Tri-bank initiative 6. Vocalink - Mastercard Trace and Prevent 7. (United States) 314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b) 8. (United States) The Duality AML Information Sharing Network in partnership with Oracle 9. (United States) Money Services Business Industry Negative Database (MSB-IND) 10. (United States) Verafin information sharing, operating under USA PATRIOT Act 314(b) 11. (Switzerland) Swiss AML Utility 12. (Singapore) COSMIC FI-FI Information Sharing Platform 13. (Netherlands) Transactie Monitoring Nederland (TMNL) 14. (Estonia) Salv - AML Bridge 15. (Australia) Australian Financial Crimes Exchange Ltd (AFCX)

[124] Future of Financial Intelligence Sharing (FFIS) A Survey and Policy Discussion Paper: "Lessons in private-private financial information sharing to detect and disrupt crime" July 2022 and FATF PARTNERING IN THE FIGHT AGAINST FINANCIAL CRIME DATA PROTECTION, TECHNOLOGY AND PRIVATE SECTOR INFORMATION SHARING, July 2022

5 Conclusions

The current guidelines aim to provide current regional threats and trends for online fraud and criminal money flows on the Internet at national and international level. These threats and trends receive a series of considerations, recommendations and conclusions that could be adopted regionally and, on a country-by-country basis, to continue to build their capability.

These comments, recommendations and conclusions relate to several stakeholders, which will require collaboration and coordination to implement.

5.1 FATF Recommendations

The FATF Recommendations, set an international standard, which countries should implement through measures adapted to their circumstances. The FATF Recommendations[125] set out the essential measures that countries should have in place to undertake AML and CFT.

Countries in Eastern Partnership region are regularly monitored and assessed as to their fulfilment and implementation of the FATF standards. Almost all the countries have been evaluated several times with the earliest report dated from 2014, but with some follow-up reports through the period where some of the weaknesses are correct. It is critical that project priority countries implement the recommendations included in the most recent evaluations.

5.2 Regional Recommendations and Comments

5.2.1 Cybercrime investigation capacity building

Implementation of a unified national online cybercrime and fraud reporting platform in each country. The creation of this portal should be used as the only reporting application for online fraud in each country. It will bring benefits for the collective LEA response against cybercrime and online fraud in the countries by producing clearer statistics regarding the threats and challenges, information that will allow trends and threats to be identified and appropriate infrastructure alongside the reporting platform will enable a more joined response in each country.

Statistical collection and analysis of data related to cybercrime, cyber-enabled crime and forensic examinations of digital devices should be implemented in each country throughout the Eastern Partnership region, to identify threats, trends, and challenges. Data should be amalgamated from LEA and CERT, to provide the best possible overview of the current situation and allow for changes to be managed. Such data can underpin and support requests to increase capacity and capability resourcing.

LEA in the region should move away from a constantly centred response of reactive investigations to one that includes more pro-active and preventative strategies. Prevention and awareness are mentioned throughout this document and innovative improvements would be useful, for example the creation of a dedicated website such as the UK Get Safe Online.[126] Proactive strategies include the use of OSING, informants, dedicated online activities into dark web sites to identify local threats and suspects, which should support investigations and knowledge growth.

[125] Set of 40 Recommendations (R1,…R40)

[126] https://www.getsafeonline.org

The development of a more structured workforce, with institutional capability to deal with cybercrime and online fraud should expand in cybercrime units and in mainstream police units (such as regional units). As the judicial process confronts more cybercrime, online fraud, and electronic evidence, it is necessary to prepare the LEA, prosecutors, and judiciary for these changes more proactively through the implementation of planned strategies supported by senior managers.

5.2.2 Financial Investigation capacity building

The number of confiscations across the region is still low. The countries from the Eastern Partnership region need to raise awareness within decision makers to agree an appropriate approach at national level for financial investigation, freezing, seizure, confiscation, and management of online assets in practice. A method of improving this position is to raise the profile of confiscations through the implementation of a strategic directive to LEA and Prosecutors. Performance Indicators should be used to identify the value of confiscations, supported with further investment of resources to increase cases and forfeitures year-on-year.

Developing parallel financial investigation strategies in all serious crime cases and including significant online fraud reports is needed throughout the region. The use of parallel financial investigations in this way will add value to complex and serious investigations, develop evidence against sophisticated criminals and support dismantling of their infrastructure. It will contribute to a more effective system, which will enable high levels of confiscation from criminals.

Develop an effective capability to investigate, search and seize cryptocurrencies (see training at 5.2.5 below).

The creation of a central system to manage seized and confiscated property should be considered across the region. This would provide an integrated response to asset recovery through developing inter-agency cooperation at national and international levels. As an example, the Romanian National Agency for the Management of Seized Assets is a useful case study.[127]

5.2.3 Online fraud awareness and prevention

More effort is needed in the region to raise financial awareness to promote financial literacy as a public value and encourage changes to people’s behaviour. Developing financial education platforms where public can be informed about different online frauds is in progress across the region. Such platforms should seek to be interactive and innovative in the provision of awareness campaigns. For examples, presenting information in the forms of publication, blogs, brochures, infographics, and short videos could have a greater impact in explaining the threat online fraud or to explain the public role of the money mule and consequences.

[127] https://anabi.just.ro/en

5.2.4 **AML/CFT awareness and prevention**

Developing new typologies and indicators that can identify online fraud and detect criminal money flow through all relevant stakeholders, with emphasis to raise the awareness and reporting from non-financial entities like DNFBP. Further decline on the number of defensive or low quality STR will be more advantageous to countries in the region.

Working together with private sector from each country should develop in-country methodology and implement tools for near real-time assessment of the risk of online fraud and criminal money flow in the financial sector. Some common indicators and measures can be found in Annex A of this report as a baseline to identify high-risk or suspicious activities and transactions.

One of the most effective measures to combat online fraud is that financial institutions need to establish processes to cool-of or delay mechanism where transactions have a high-risk score[128] related to online fraud or criminal money flow.

Countries from the region should implement innovative technological analytical solution that support their activities for timely detection and disruption of the criminal money flow. Investigators should be trained for new types of online fraud, new threats, trends, typologies, technologies, and standards.

Efforts need to be paid to sustain continuous and consistent multilateral cooperation and coordination mechanisms dedicated to problem identification at AML/CFT system level and the adoption of proactive and/or reactive policies to cope with new emerging issues.

Enhanced public-private co-operation and information exchange at the national, regional, and international level is consider desirable.

Through private-private collaboration platforms, it is possible to achieve more consistent *financial exclusion decisions against fraudsters and high-risk entities*. Potentially this should support real-time identification and interdiction of the proceeds of crime flowing across multiple financial institutions – and even across borders. It is possible to re-orient the AML framework from being focused on collecting a vast record of historic suspicious transactions, to being an intelligence-led public -private and private-private collaborative effort to dismantle crime networks. For more information on private-private collaborations, see Annex B.

5.2.5 **Training**

The implementation of training strategies is necessary across the region. Guidance is provided in the Council of Europe Guide for Developing LEA Training Strategies on Cybercrime and Electronic Evidence.[129] The setting up of structure, building teams and implementing training should be organised so the right staff are trained and retained in the respective units to build a more sustainable response to cybercrime, online fraud and handling electronic evidence.

[128] See Annex A on how to compute transaction risk score.

[129] https://rm.coe.int/guide-for-developing-training-strategies-final/1680a62c72

The search, seizure and confiscation of cryptocurrencies is a growing area of concern for LEA across the world. Capacity building and training is needed amongst LEA and the judiciary to understand fundamentals of how to investigate the blockchain, engage with service providers and utilise appropriate methodology to seize the different types of cryptocurrencies. Such training and investigation need to be supported with a software solution that supports the fast and efficient investigation of the blockchain (Graphsense[130] or Chainalyisis[131] are examples of such solutions). The capacity building and training should consider the Council of Europe Guide on Seizing Cryptocurrencies.[132]

Develop adequate skills and equip with necessary resources officers in the FIU and LEA OSINT techniques so they can monitor the online environment for online frauds, conduct blockchain analytics to implement the follow the money principle and supplement the seizing of online assets.

5.3 Country Recommendations and Comments

5.3.1 Armenia

The creation of a dedicated National Cyber-Security Strategy is necessary to put in place structured plans to improve the security and resilience of infrastructures and services in Armenia. The strategy should set out national objectives and priorities, with supporting action plans so that these can be achieved in a specified timeframe. The strategy should either include, or set out separately, the national objectives and priorities for dealing with cybercrime and online fraud.

It is apparent that LEA in Armenia have difficulties in turning financial intelligence into tangible evidence, which underlines the need for more training of LEAs on investigative matters.

AML cooperation between the FIU and LEA is a good source of intelligence for ML/FT purposes for LEA. Information can be exchanged rapidly and securely between the relevant authorities spontaneously and upon request. In Armenia some limitations need to be eliminated on the ability of the LEA to routinely request financial intelligence from the FIU, which can have negative impact on inter-agency cooperation to combat with online fraud as predicate offence.

5.3.2 Azerbaijan

The Code of Criminal Procedure should be updated to include reported gaps to accord more fully with the Budapest Convention on Cybercrime.

Qualified review and improvement of the Criminal Code and Code of Criminal Procedure is necessary to ensure that it has sufficient legal framework to support financial investigations in criminal proceedings. Additional improvements should ensure definitions that criminal property

[130] https://graphsense.info

[131] https://www.chainalysis.com

[132] https://www.coe.int/en/web/cybercrime/-/iproceeds-2-guide-on-seizing-cryptocurrencies-available-on-the-octopus-cybercrime-community

includes non-tangible assets when considering money laundering. This definition needs inclusion into the legal framework to support advances in the search, seizure, and confiscation of online criminal assets such as cryptocurrencies.

Seizure and Confiscation of the criminal proceeds are in place in the legal framework, however further strengthening should be considered to allow non-conviction-based confiscation in Azerbaijan.

5.3.3 **Georgia**

AML cooperation between the FIU and LEA is a good source of intelligence for ML/FT purposes for LEA. Information can be exchanged rapidly and securely between the relevant authorities spontaneously and upon request. In Georgia some limitations need to be eliminated on the ability of the LEA to routinely request financial intelligence from the FIU, which can have negative impact on inter-agency cooperation to combat with online fraud as predicate offence.

Measures for the postponement of transaction need to be further examined in Georgia to prevent timely dissipation of the assets gathered through online fraud through the traditional banking system. Seizure and confiscation of the criminal proceeds are in place in the legal framework, however further strengthening should be consider in a form of policy, to widen the use of non-conviction-based confiscation in Georgia.

5.3.4 **Moldova**

The Criminal Code and Criminal Procedure Codes appears to provide no definitive clarification that property includes non-tangible assets when considering money laundering within the Criminal Code or Criminal Procedure Code. This is especially relevant when considering the search, seizure and confiscation of criminal assets acquired in online fraud or cybercrime. Further clarification that the definition provided in the AML/CFT legislation applies to other parts of the legal framework to support advances in the search, seizure, and confiscation of online criminal assets, such as cryptocurrencies, appears necessary.

5.3.5 **Ukraine**

The delivery of this recommendations may be postponed until a more suitable time considering the current situation in Ukraine, who have been invaded by the Russian Federation. But the recommendations are set out for information of decision makers.

The dedicated National Cyber-Security Strategy of Ukraine has expired. Further update is necessary to put in place structured plans to improve the security and resilience of infrastructures and services in Ukraine. The strategy should set out national objectives and priorities, with supporting action plans so that these can be achieved in a specified timeframe. The strategy should either include, or set out separately, the national objectives and priorities for dealing with cybercrime and online fraud. It is likely that any national strategy would focus upon the national security situation, but considerations for cybercrime are still valid.

The Criminal Code and Criminal Procedure Codes provide no definitions that property includes non-tangible assets when considering money laundering. This definition needs inclusion into the legal framework to support advances in the search, seizure, and confiscation of online criminal assets such as cryptocurrencies.

ANNEX A

(4.3.2 Preventive measures to combat online fraud activity)

1. Implementation on centralised transaction databases that can be used to correlate transactions, perform analysis, identify suspicious transactions, create typologies related to the online fraud, create risk indicators, and rapidly detect criminal activity both within a financial institution and between financial institutions (see chapter 4.6.5. Private Partnership);

2. Perform Behavior profiling of the client monitoring for the abnormal behavior on the clients' accounts in financial institutions (unusual pattern of spending, unusual time of transaction, unusual beneficiary account);

3. Monitor and alert on change of beneficiary bank account (IBAN), where transaction between two companies have been carried out through bank accounts mentioned in the purchase agreement and especially where beneficiary is in distant time zone;

4. "Blacklisting" of known or suspected accounts [133] (intermediary or beneficiary account);

5. Implementation of protective system in the financial institution based on AI tools that help compute transaction risk score[134] in near real time;

6. Checking the pattern of frequent "Impossible Travel"[135] pattern in client online activity;

7. Check the documents for Know Your Customer (KYC), if they appear to be forged, falsified, or stolen. Sometimes documents that are forged or stolen may be almost impossible to distinguish from legitimate documents because there are KYC kits present on the Darknet markets;

8. Monitor if groups of foreign nationals open large numbers of accounts simultaneously and have no clear link to the country where the financial institution operate;

9. Monitor if numerous individuals open accounts within a short period using shared addresses, mobile devices, IP addresses and other common identity indicators;

10. Monitoring customer devices to identify whether multiple customers are using the same mobile device, IP addresses and other common identity indicators to access their accounts;

11. Ask more context for the transaction whether, account holder not have any understanding of what the funds in the account are being used when questioned. In a case of stolen identity, they may not even be aware that an account has been opened in their name;

[133] Blacklisting of account is potentially leading to individual's financial exclusion from the financial institution (due to the high ML risk)

[134] Transaction risk score in online environment can be compute as mathematic algorithm depended on several factors: detection of malware on client device, present spyware in the communication session, no integrity of the device, no certain level of security patches on a device and many more.

[135] Impossible Travel is a calculation made by comparing a user's last known location to their current location, then assessing whether the trip is likely or even possible in the time that elapsed between the two measurements.

12. Check if the mule accounts feature some randomly generated email addresses that just have a string of random numbers and letters;

13. Searching customer accounts for signs of emails registered to foreign domains inconsistent with their residential addresses;

14. Ask more context for the transaction whether, some mules may suggest that they have responded to ads on social media platforms offering money to open an account at the exchange;

15. Check whether multiple customers make high-value onward transfers to common accounts in high-risk jurisdictions with no clear apparent purpose;

16. Monitoring and analysis of card transaction, especially pattern of cash withdrawal from the bank accounts through various ATMs within short period of time ;

17. Monitoring online and card transactions and seek links through the online/card accounts where the value has transferred especially when destination is high risk for ML[136].

18. Monitoring on Fiat funds may be sent to the VASP (crypto exchange) from corporate bank accounts – suggesting an online banking compromise – with requests to make rapid high-value transfers into crypto assets;

19. Use crypto asset transaction monitoring software to identify transactions among customers that demonstrate patterns of money mule activity;

20. Limiting the amounts of funds that can be transferred using online accounts and cards;

21. Implementing specific measures adopted by payment card industry that include implementation of security standards by merchants, processors, and financial institution[137] or risk management guides for merchants;

22. Information sharing between financial institutions and threat intelligence sharing through meetings on specialised working group or expert committee in banking association or through CSIRT;

23. Following the FS-ISAC[138] or other financial sector CSIRT or public/private cooperation for threat intelligence and timely issue an advisory on fraud for corporate clients or individuals.

[136] Ex. High risk VASP platform working with privacy coins or in (Identification of such card transaction can be detected through MCC code of the merchant, who is beneficiary of the e-commerce transaction (crypto asset card transaction ex. MCC 6051 – Quasi Cash)

[137] Such as the Payment Card Industry Data Security Standard (PCI DSS) and related requirements https://www.pcisecuritystandards.org/security_standards/index.php

[138] "Financial Services – Information Sharing and Analysis Center" (FS-ISAC) is a US industry forum for co-operation on critical (physical and cyber) security threats to the financial sector. It collects and analyses information and alerts from member organisations of threats and attacks to help the financial services sector to prepare and respond to threats.

ANNEX B

Partnering in the fight against financial crime

(4.6.5. Private-Private information exchange)

AML Bridge (Estonia):

Post-suspicion private-private information sharing initiative Use case: AML Bridge is a secure digital platform provided by an independent third-party company. It allows member banks to exchange pseudonymised data (largely transaction data) with one or more other banks in an end-to-end encrypted format. The list of receiving institutions is defined individually by each member for each exchange. Information is shared on a near-to real-time basis to pursue collaborative investigations.

Intended outcomes/results or achieved results;

- As of March 2022, AML Bridge has seen 1200 private-private 'collaborative investigations' completed since it was established in July 2021 (~150 cases per month);
- Half of these cases (over 600) involved ML investigations, which has increased the quality of STRs submitted, including by promoting joint STRs. These cases have also helped to clear non-suspicious customers more quickly (i.e., reduce false positives);
- One third of the cases (over 400) relate to 'scam fraud', which generally means a form of authorised push payment (APP) fraud. Approximately EUR 3 million has been recovered from criminals and returned to victims with the help of AML Bridge. For fraud, speed is key, and AML Bridge enables most of the urgent cases to be resolved in under 15 minutes;
- Collaborative investigations related to sanctions evasions were initially a small category. However, following Russia's invasion of Ukraine (in March 2022) these cases account for most of the AML Bridge usage, with weekly volumes quadrupling over the course of March 2022. The dominant use case is quickly clearing new exact-match false positives, which are overwhelming sanctions teams and frustrating good customers. In addition, the network is observing opportunities to start sharing and spreading information about close associates and owned companies of sanctioned persons and entities.

Participants:

The AML Bridge platform is provided by an independent third-party company (a 'data processor' under the GDPR). AML Bridge was first launched between four of Estonia's largest banks (collectively representing 90% of transactions) and has since expanded to include all 10 Estonian banks and several non-banks in the country.

A range of individuals and teams within the banks play critical roles in the project, including CEOs (executive support), MLROs (Steering Committee members), Data Protection Officers (advisors), information security teams (to ensure a secure platform for sharing). In addition, each bank appoints project leads who attend the Steering Committee, act as the first point of contact between the platform provider/data processor and the bank, and co-ordinate internally. The end-users of the AML Bridge are the bank 'crime fighting' teams (AML/CFT/CPF, sanctions screening, transaction monitoring, anti-fraud, etc.) who run the operational work and provide constant feedback on the platform.

Specific data points collected/shared:
The data shared is mostly transaction data and is shared on a near-to real-time basis. The exact structure of shared data is configurable and determined based on the suspected offence and the individual network members. Sharing using "scenario templates" allows participants to define the input fields required for the recipient to identify the subject (e.g., customer name, account number, transaction ID) and the requested specific data (e.g., full name, date of birth, source of wealth, payment reason, risk level, potential red flags, copies of the documents, etc.). Data sharing covers investigations/enquiries around potential ML, sanctions evasion, fraud, and related incidents.

Lawful basis for processing personal data:
As the controllers of the data, each bank must have a legal basis to share data through the AML Bridge platform. In most cases, the banks will share and process information on one of two grounds under the GDPR: 'compliance with the law' or 'legitimate interest' (GDPR, Article 6.1(e)). In addition, Estonia's ML/TF Prevention Act establishes some limitations of DPP rights of data subjects on the basis that AML/CFT/CPF activities are classified as a matter of public interest. In particular, the Act states that financial institutions are allowed to share personal data for collaboration purposes (section 16) and that, in such cases, certain privacy rights of the data subject can be restricted based on the public interest of AML/CFT/CPF activities (section 48). Each participating bank signs a Data Processing Addendum (a contract between the bank and the platform provider/data processor to protect data in compliance with the GDPR).

Assessment of proportionality:
The extent and amount of data shared its geographical scope, and its retention periods are defined by the banks using the platform. Nevertheless, the design of AML Bridge limits the amount and type of data being shared to help institutions minimise sharing; the platform has extensive audit logging to help banks conduct reviews and quality assurance checks and identify unreasonable actions.

Other DPP considerations:

- Transparency/notification and rights of data subjects: The Data Processing Addendums stipulate that the platform provider/data processor will provide all reasonable assistance to the data controller (the bank) for the fulfilment of the controller's obligation to respond to requests from data subjects exercising their data protection rights. If the platform provider/data processor receives any such requests, they are forwarded to the bank with all relevant information.
- Confidentiality/data security: The AML Bridge has an information security management system in place which includes strict access control (including Multi-Factor Authentication and IP whitelisting), encryption (in transit and at rest), disaster recovery (with backups and regular testing) and audit logs. Security documentation, including audit reports, is available to all participants. The security of the platform is tested at least annually by a qualified third party and all participating institutions have the rights to do their own penetration testing (one bank has used this right and shared the results with other participants).

Technologies utilised:
AML Bridge uses end-to-end password-based encryption. All messages are encrypted with a private plus public key pair, and to decrypt messages, the user must gain access to their private key by entering another password, which is different from their main login password. Neither the platform provider nor any other party has access to this key.

key by entering another password, which is different from their main login password. Neither the platform provider nor any other party has access to this key.

Additional considerations/challenges:

- Unclear regulations are the biggest barrier to private-to-private data sharing: Banks were only willing to start sharing information in a way that was explicitly permitted under the relevant legislation and regulations.
- The GDPR is not a barrier, but an enabler of financial crime data sharing: The consistent framework across private banks and regulators allows all participants and entities involved to quickly agree whether a particular form of private-to-private financial crime data sharing is acceptable.
- Regulators (especially supervisors and data protection authorities) must be involved from the beginning: The success of AML Bridge comes, in part, from its governance. Regulators are often adversarial with those they are regulating; this project avoided major setbacks by keeping all stakeholders not only informed but actively involved. Banks gained confidence to innovate because there was no risk of a negative surprise from the FSA or DPA.
- Within banks, executive sponsorship is a necessary precondition to kick off new data sharing initiatives: It takes significant effort from a variety of teams and individuals, across many months, to create and implement a financial crime data-sharing initiative. It must be a priority from senior bank leadership.

Involvement of authorities (AML/CFT/CPF or DPP):

Government oversight of AML Bridge is provided by the Financial Supervision Authority (which is a member and observer of the AML Bridge Steering Committee), the FIU (Steering Committee member), and the Data Protection Authority (Steering Committee observer).

Source:

Discussions with and input from AML Bridge participants, AML Bridge, available at: https://salv.com/uploads/AML-Bridge-Estonia.pdf

(APP fraud) stand for authorised push payment fraud - where an individual is deceived into sending a payment to a bank account controlled by the fraudster. Often, this occurs by the fraudster obtaining information on the victim (e.g., via access to a hacked email account) and impersonating a legitimate company with which the victim is doing business. APP fraud may also include investment or romance fraud. As the victim authorises the payment, it is often difficult or impossible to reverse/revoke the transaction.